DAVID FRIEDMAN

FUTURO IMPERFECTO

TECNOLOGIA Y LIBERTAD EN UN MUNDO INCIERTO



INNISFREE

PRIMERA PARTE: PRÓLOGO

SEGUNDA PARTE

TERCERA PARTE: HACER NEGOCIOS EN LÍNEA

VEINTIDÓS: Tiempos interesantes

BIBLIOGRAFÍA

PRIMERA PARTE

PRÓLOGO

UNO

INTRODUCCIÓN

Hace unos pocos años asistí a un evento en que el ponente invitado era un miembro del Gabinete estadounidense. Conversando después, salió el tema del suministro de petróleo a largo plazo. Me advirtió de que, llegado un punto, quizás un siglo o así en el futuro, alguien pondría la llave en el contacto del coche, lo daría, y no pasaría nada: no habría gasolina.

Lo que me impactó no fue su ignorancia sobre la economía de los recursos no renovables (si alguna vez nos quedamos sin gasolina, se tratará de un proceso largo y lento de precios en alza continua), sino el increíble conservadurismo de su visión del futuro. Era como si un funcionario similar, cien años antes, hubiera advertido de que para el año 2000 las calles estarían tan saturadas por los desechos de los caballos que serían intransitables. Pero no es probable que sea un sitio en el que el proceso de ir de aquí hacia allá comience colocando una llave en el contacto, girándola, y arrancando un motor de combustión interna quemando gasolina.

Este libro surgió de un seminario de tecnologías del futuro que impartí durante ciertos años en la facultad de Derecho de la Universidad de Santa Clara. Todos los jueves discutíamos una tecnología de la que estaba dispuesto a argumentar, al menos durante una semana, que podría revolucionar el mundo. El domingo, los estudiantes me mandaban por correo asuntos legales que podría plantear esa revolución, para que luego se subieran a la página web de la clase y la leyeran otros estudiantes. El martes discutíamos los asuntos y cómo enfrentarnos a ellos. El siguiente jueves, una nueva tecnología y una nueva revolución.

La idea del curso comenzó con dos tecnologías por entonces oscuras: encriptación de clave pública y la nanotecnología. A medida que se fue desarrollando el curso, me encontré explorando una gama considerable de otrastecnologías, con una característica en común: cada una de ellas podría cambiar el mundo durante mi vida. Lo que estás leyendo es una exploración de aquellas tecnologías, los futuros que cada una podría generar, y cómo podríamos lidiar con ellos. Este capítulo investiga brevemente las tecnologías; el siguiente discute el problema de ajustar nuestras vidas e instituciones a sus consecuencias.

En este momento, el foco de preocupación acerca del futuro que está de moda es el calentamiento global. Seguramente es un problema real y, quizás, en algún momento se debería hacer algo al respecto. Pero, a pesar de toda la furia pública y las imágenes de ciudades inundadas, según las pruebas actuales no es un problema muy grande. Las últimas estimaciones del IPCC [Grupo Intergubernamental de Expertos sobre el Cambio Climático] predicen, si no se hace nada, un aumento del nivel del mar de treinta o sesenta centímetros, y quizás un pequeño aumento en la frecuencia y fuerza de los huracanes. Es posible que esas predicciones resulten ser demasiado modestas, pero es con lo que tenemos que trabajar ahora.

Al menos tres de las tecnologías que discuto en este libro (nanotecnología, biotecnología e inteligencia artificial [IA]) tienen el potencial de barrer a nuestra especie mucho antes de finales de siglo. También tienen el potencial de crear un futuro suficientemente rico y avanzado tecnológicamente para hacer del calentamiento global un problema que puede solucionarse al coste de la limosna de unos pocos filántropos. Otras tecnologías podrían crear futuros impactantemente diferentes al presente de una amplia variedad de maneras: una sociedad radicalmente más o radicalmente menos libre de aquella en la que vivimos ahora, más privacidad de la que los humanos hayan conocido jamás, o menos, humanos viviendo como dioses o como esclavos. Sus consecuencias afectarán no solo a la ley, sino al matrimonio, cuidado de los hijos, instituciones políticas, negocios, vida, muerte y mucho más.

No soy un profeta; cualquiera de estas tecnologías que discuto podrían prometer mucho y luego ser un fiasco. Solo hace falta que una no lo sea para rehacer el mundo. Observar algunas candidatas nos preparará algo mejor si una de esas revoluciones resulta ser real. Quizás más importante, después de haber pensado sobre cómo adaptarnos a cualquiera de las diez revoluciones posibles, al menos tendremos terreno ganado cuando nos surja la undécima de repente. La conclusión que quiero que saquen de este libro los lectores no es que cualquiera de los futuros que dibujo vaya a pasar. La conclusión que quiero que saquen es que el futuro es radicalmente incierto. De maneras interesantes.

Y que merece la pena empezar a pensar en las posibilidades, y en cómo encararlas, ahora mismo.

Futuros posibles

Comenzamos con tres tecnologías pertinentes a la privacidad: una que la incrementa radicalmente, la otra que la disminuye de forma extrema.

Privacidad x3 o Ahora la tienes, ahora no

La encriptación en clave pública posibilita la comunicación irrastreable inteligible solo para el receptor deseado. Mi firma digital demuestra que soy la misma identidad en línea con la que trataste ayer y con la que trató tu compañero el año pasado, sin necesidad de que ninguno de los dos conozcáis detalles tan irrelevantes como edad, sexo o en qué continente vivo. La combinación de la red informática y la encriptación en clave pública hace posible un nivel de privacidad nunca antes conocido por los humanos, un mundo en línea donde la gente tiene tanto identidad como anonimato. A la vez. Una implicación es la libertad de expresión protegida por las leyes de la matemática, posiblemente más digna de confianza y ciertamente con una

jurisdicción más amplia que la del Tribunal Supremo. Otra es la posibilidad de empresas delictivas con reputación de marca: archivos piratas en línea vendiendo la propiedad intelectual de otras personas por un céntimo cada dólar, agencias de trabajo temporal contratando los servicios de falsificadores y asesinos a sueldo.

Por otra parte…

En el futuro no tan lejano podrías ser capaz de comprar una videocámara barata con las características de tamaño y aerodinámica de un mosquito. Incluso antes, veremos (ya estamos viendo) la proliferación de cámaras en farolas diseñadas para evitar delitos. En última instancia, esto podría llevar a una sociedad donde nada es privado. El escritor de ciencia ficción David Brin ha argumentado que la mejor solución disponible no será la privacidad, sino la transparencia universal: un mundo donde todos pueden vigilar a los demás. La policía te está vigilando, pero alguien los está vigilando a ellos.

Una ciudad solía ser más privada que un pueblo, no porque nadie pudiera ver lo que hacías, sino porque nadie podía seguir el rastro de lo que todos estaban haciendo. Este tipo de privacidad no puede sobrevivir al procesamiento de datos moderno. El ordenador en que estoy escribiendo estas palabras tiene suficiente capacidad de almacenaje para guardar al menos una modesta cantidad de información sobre todo ser humano de Estados Unidos y suficiente poder de procesamiento para localizar rápidamente a cualquiera de ellos por nombre o características. De ese hecho surge el problema de quién tiene qué derechos respecto a la información sobre mí que se encuentra actualmente en las manos y mentes de otra gente.

Junta todas esas tecnologías y podríamos terminar en un mundo donde tu identidad en el espacio real sea completamente pública, donde se sabe todo sobre ti y esa información es fácilmente accesible, mientras que tus actividades ciberespaciales y la información sobre ellas

son totalmente privadas y donde tú estás al mando del enlace entre tu imagen ciberespacial y tu identidad en el mundo físico.

Comercio en el ciberespacio

El mundo que crean la encriptación y las redes sociales requiere una manera de realizar pagos, idealmente sin tener que revelar la identidad del que paga o el receptor. La solución, con la que ya se ha dado en teoría pero todavía no se ha implementado totalmente, es el ecash: dinero electrónico, producido de forma privada, potencialmente irrastreable. Una consecuencia menor es que las leyes de blanqueo de dinero se vuelven inejecutables, ya que se pueden transferir grandes cantidades de dinero simplemente mandando un correo al receptor.

Un mundo de privacidad férrea requiere alguna manera de acuerdos de ejecución legal: ¿cómo denuncias a alguien por romper un contrato cuando no tienes ni idea de quién o qué es él o ella, o dónde está? Este y otros problemas relacionados nos llevan a una tecnología legal en que las reglas legales se crean de forma privada y se ejecutan mediante sanciones de reputación. Es una tecnología antigua, que se remonta al menos a la Lex Mercatoria,ejecutada privadamente, a partir de la que las leyes comerciales modernas evolucionaron[1]. Pero para la mayor parte de los lectores modernos, incluyendo a la mayoría de los abogados y profesores de Derecho, será nuevo.

La propiedad en línea es en gran parte propiedad intelectual, lo que plantea el problema de cómo protegerla en un mundo donde la ley de derechos de autor se está volviendo inejecutable. Una posibilidad es sustituir la protección tecnológica por protección legal. Un programa o una base de datos viene dentro de una pieza de software (Intertrust lo llamó una digibox o «digicaja») que regula su uso. Ejecutar el programa o usar la base de datos cuesta diez céntimos de dinero electrónico,

[1] Benson, 1989, pp. 644-661; http://garnet.acns.fsu.edu/~bbenson/.

transmitidos instantáneamente por la red al propietario de los derechos de autor.

Por último, y quizás lo más radical, un mundo de comunicación fácil y barata facilita enormemente el acceso descentralizado a la producción. Un resultado posible es convertir cantidades sustanciales de esfuerzo humano a partir del contexto de corporaciones jerárquicamente organizadas en alguna mezcla de coordinación de mercado de individuos o pequeñas empresas y el tipo de cooperación voluntaria, sin mercados explícitos, de la que el desarrollo de software de código abierto es un ejemplo reciente e impactante.

Delito, polis y ordenadores

Algunas tecnologías dificultan el trabajo de la ejecución de la ley. Otras lo hacen más fácil, incluso demasiado. Unos pocos años atrás, cuando el proyecto de ley sobre las escuchas telefónicas digitales pasaba por el Congreso, los críticos señalaron que la capacidad que el FBI estaba exigiendo que le proporcionaran las compañías telefónicas ascendía a la capacidad de pinchar más de un millón de teléfonos. Simultáneamente.

Todavía no sabemos si tienen la intención de hacerlo, pero se está volviendo cada vez más claro que si quieren, pueden. El mayor coste de una escucha telefónica es la mano de obra. A medida que mejora el software diseñado para permitir que la gente dicte a sus ordenadores, ese alguien puede ser un ordenador convirtiendo conversaciones en texto, buscando en el texto palabras clave o expresiones, e informando de si las ha encontrado a un humano. Los ordenadores trabajan barato.

Además de proporcionar a la policía nuevas herramientas para ejecutar la ley, los ordenadores plantean numerosos problemas para definir y evitar los delitos. Piensa en la pregunta de cómo debería clasificar la ley un «asalto por ordenador», que consiste, no en alguien asaltando de verdad algún sitio, sino en un ordenador mandando

mensajes a otro y recibiendo mensajes como respuesta. O plantéate el potencial para aplicar la clásica técnica salami (robar una cantidad muy pequeña de dinero de muchas personas) en un mundo donde decenas de millones de personas unidas a Internet tienen software en sus ordenadores diseñado para pagar facturas en línea.

Niños diseñadores, vida larga y cadáveres crionizados

Las tecnologías de nuestro próximo grupo son biológicas. Dos (el control de paternidad y la fecundación in vitro) ya han abolido varios de los hechos en que se basaban los últimos mil años del derecho familiar. Ya no es simplemente un hijo sabio el que conoce a su padre: cualquiera puede, si se le da acceso a muestras de tejido y a un laboratorio decente. Ya no es el caso que una mujer de cuyo cuerpo nace un niño sea necesariamente su madre. La ley ha comenzado a amoldarse. Una pregunta interesante que todavía queda es hasta qué grado reestructuraremos nuestro patrón de apareamiento para aprovecharnos de los cambios en la tecnología de producir bebés.

Un poco más adelante en el futuro se encuentran las tecnologías que nos proporcionan control sobre la herencia genética de nuestros hijos. Mi favorita es la eugénica libertaria dibujada décadas atrás por el autor de ciencia ficción Robert Heinlein: tecnologías que permiten que cada pareja elija, de entre los niños que podrían tener, cuáles quieren, eligiendo el óvulo que no lleva la tendencia de la madre a la miopía para combinarse con el espermatozoide que no lleva la herencia del padre de un corazón malo. Haz este proceso a lo largo de cinco o diez generaciones participando una fracción aceptable de la población y obtienes un cambio sustancial en el acervo de genes humanos. De forma alternativa, si se aprende lo bastante para realizar ingeniería genética de copiar y pegar, los padres pueden olvidarse de la espera y realizar todo el trabajo en una generación.

Ahora salta del comienzo de la vida al final. Dada la tasa de progreso en el conocimiento biológico durante el pasado siglo, no hay razón para dar por hecho que el problema del envejecimiento seguirá siendo insolucionable. Porque la recompensa no solo es enormemente grande, sino que también es más inmediata a los que son actualmente viejos, algunos de los cuales también son ricos y poderosos: si puede solucionarse es probable que se solucione.

En cierto modo ya se ha hecho. Actualmente hay más de cien personas cuyos cuerpos no están envejeciendo porque están congelados, mantenidos a la temperatura del nitrógeno líquido. Todos ellos están legalmente muertos. Pero su esperanza al fijar su estado actual era que no sería permanente, que con suficiente progreso médico algún día será posible revivirlos. Si comienza a parecer que van a ganar la apuesta, tendremos que pensar seriamente en adaptar las leyes e instituciones a un mundo donde haya un estado intermedio entre vivo y muerto y en el que se encuentre mucha gente.

La verdadera ciencia ficción

Por último, llegamos a tres tecnologías cuyos efectos, si tienen lugar, son lo suficientemente extremos para que todo pueda ser posible, pues podrían provocar tanto la extinción como la alteración radical de las posibilidades reales de nuestra especie dentro del lapso de vida de la mayor parte de la gente que lee este libro.

Una de esas tecnologías es la nanotecnología, la capacidad de construir objetos a escala atómica, construir máquinas cuyas partes sean átomos sencillos. Esta es la forma en que se construyen cosas vivientes: una hebra de ADN o una enzima es una máquina molecular. Si nos volvemos lo bastante buenos trabajando con objetos muy pequeños para hacerlo por nosotros mismos, las posibilidades van desde máquinas reparadoras de células microscópicas que vayan por un cuerpo humano arreglando todo lo que esté mal hasta criaturas

microscópicas autorreplicantes dedicadas a convertir todo el mundo en copias de sí mismas (conocidas en los círculos nanotécnicos como el marco hipotético de la «plaga gris»).

La inteligencia artificial podría superar a la nanotecnología en las probabilidades de aniquilación o en crear un paraíso terrenal. Raymond Kurzweil, muy enterado de los ordenadores, estima que en unos treinta años habrá ordenadores programados con inteligencia al nivel de la humana. A primera vista, esto sugiere un mundo de robots de ciencia ficción y, si tenemos suerte, que nos obedezcan y hagan el trabajo sucio. Pero si en treinta años los ordenadores son tan inteligentes como nosotros y si las tasas de mejora actuales (para los ordenadores, pero no para los humanos) continúan, significa que en cuarenta años estaremos compartiendo el planeta con entes al menos más inteligentes que nosotros que nosotros frente a los chimpancés. La solución de Kurzweil es que nosotros también nos volvamos más inteligentes, aprender a hacer en silicio parte de nuestro pensar. Ello podría proporcionarnos un mundo muy extraño: poblado por humanos, con combinaciones humano/máquina, máquinas programadas con los contenidos de una mente humana que se piensa que son ese humano, máquinas que han evolucionado su propia inteligencia y mucho más.

La última tecnología es la realidad virtual (VR). Las versiones presentes la abordan con la fuerza bruta: imágenes proporcionadas a ojos y oídos mediante gafas y cascos. Pero si podemos dar con el problema de soñar, descubrir cómo nuestro sistema nervioso codifica los datos que llegan a nuestras mentes en forma de percepciones sensoriales, ya no harán falta gafas ni cascos. Enchufa un cable en un enchufe detrás del cuello para obtener una percepción mediante todos los sentidos de una realidad observada con sensores mecánicos, generada por un ordenador o grabada de otro cerebro.

Los beneficios inmediatos son que el ciego verá (a través de videocámaras) y el sordo oirá. La consecuencia a mayor plazo podría ser un mundo donde casi todo lo importante consista en señales moviéndose de un cerebro a otro por una red, donde los actos físicos

realizados por cuerpos físicos representen un papel menor. Para visitar a un amigo de Inglaterra no hace falta mover ni su cuerpo ni el mío: estar ahí es tan fácil como marcar el teléfono. Esta es una de las muchas razones por las que no espero que los automóviles movidos por gasolina representen un papel importante en el transporte dentro de un siglo.

Unas pocas páginas atrás estábamos estudiando un mundo donde el espacio real fuera completamente público, el ciberespacio completamente privado. Tal y como están las cosas ahora, sería un mundo muy público, ya que la mayor parte de nosotros vive la mayor parte de nuestras vidas en el espacio real. Pero si la realidad virtual profunda nos proporciona un mundo donde todo lo interesante ocurre en el ciberespacio y la actividad en el espacio real consiste en poco más que mantener vivos nuestros cuerpos, podría ser un mundo muy privado.

Habiendo llamado a esta sección ciencia ficción, no puedo resistirme a añadir un capítulo sobre las maneras en que las tecnologías actuales y de un futuro próximo podrían posibilitar el antiguo sueño de la ciencia ficción: viajes espaciales, habitantes espaciales y, quizás, con el tiempo, las estrellas.

Alternativas

Cualquiera de los futuros que he dibujado podrían tener lugar, pero no todos. Si la nanotecnología convierte el mundo en plaga gris en 2030, también convertirá en plaga gris los ordenadores en los que se habría desarrollado las superinteligencias artificiales. Si la nanotecnología se atasca y la inteligencia artificial no, los ordenadores programados que dirigen el mundo de 2040 podrían estar más interesados en sus propias visiones sobre cómo debería evolucionar la especie humana que en nuestra visión de qué tipo de hijos queremos tener. Y, yendo más cerca de casa, si se construye la encriptación privada fuerte en nuestros sistemas de comunicación, con la

encriptación y la desencriptación bajo el control no de la red, sino de los individuos comunicándose los unos con los otros (la pesadilla de la Agencia de Seguridad Nacional durante los últimos veinte años o así), no importará cuántas líneas de teléfono pueda pinchar el FBI.

Esta es una razón por la que este libro no es una profecía. Espero que sucedan partes de lo que describo, pero no sé cuáles. Mi propósito no es predecir qué futuro conseguiremos, sino usar futuros posibles para pensar en cómo el cambio tecnológico nos afectará y cómo podemos y deberíamos cambiar nuestras vidas e instituciones para adaptarnos a él.

También hay una razón por la que, con unas pocas excepciones, he limitado mi discusión del futuro a los próximos treinta años o así. Es aproximadamente el punto en que tanto la inteligencia artificial como la nanotecnología comenzarán a ser de importancia. También está lo bastante lejos para permitir que las tecnologías que todavía no han llamado mi atención comiencen a representar un papel importante. Más allá de eso, mi bola de cristal, muy borrosa en el mejor de los casos, se vuelve inútil; el futuro más lejano se disuelve en la niebla.

DOS

VIVIENDO CON EL CAMBIO

Las nuevas tecnologías cambian lo que podemos hacer. A veces facilitan lo que queremos hacer. Tras escribir un libro con un procesador de texto, uno se pregunta cómo se hizo alguna vez sin uno. A veces facilitan lo que otro está haciendo y nos dificultan evitar que lo haga. Ejecutar la ley de derechos de autor se volvió más difícil cuando la fotocomposición tipográfica hizo el coste de producir una edición pirata más bajo que el de la edición autorizada contra la que competía, y de nuevo más difícil cuando la copia barata puso las herramientas de la piratería en las manos de cualquier profesor universitario que busca material de lectura para sus estudiantes. A medida que los micrófonos y las videocámaras se hicieron más pequeñas y baratas, evitar que otra gente me espíe se vuelve más difícil.

La respuesta obvia es intentar seguir haciendo lo que hemos estado haciendo. Si es más fácil, bien. Si es más difícil, lo siento. El mundo debe seguir, la ley debe ejecutarse. Que se haga justicia, aunque se caiga el cielo.

Obvio y equivocado. Las leyes que tenemos, las maneras en que hacemos las cosas, no se nos entregan del cielo en tablas de piedra. Son artilugios humanos, soluciones a problemas particulares, maneras de conseguir fines particulares. Si el cambio tecnológico dificulta la ejecución de una ley, la mejor solución a veces es dejar de ejecutarla. Podría haber otras maneras de conseguir el mismo fin, incluidas algunas posibilitadas por el mismo cambio tecnológico. La cuestión no es cómo seguir haciendo lo que hemos estado haciendo, sino cómo conseguir mejor nuestros objetivos bajo nuevas circunstancias.

Si este libro tiene una temática, es esa.

Un ejemplo simple: la muerte de los derechos de autor

La ley de los derechos de autor le da al autor de una obra sujeta a ellos el derecho a copiarla. Si copiar un libro requiere una cara maquinaria de impresión operando a gran escala, ese derecho es razonablemente fácil de ejecutar. Si todo lector posee un equipo que puede realizar una copia perfecta de un libro a un precio insignificante, ejecutar la ley se vuelve casi imposible.

En lo que respecta al material impreso, la ley de derechos de autor se ha vuelto menos ejecutable durante el pasado siglo, pero todavía no es inejecutable. Las copiadoras a las que la mayor parte de nosotros tenemos acceso pueden reproducir un libro, pero el coste es comparable al de comprar el libro y la calidad es peor. La ley de derechos de autor en obras impresas todavía se puede ejecutar, incluso si es menos fácil que en el pasado.

No se puede decir lo mismo de la propiedad intelectual en formato digital. Cualquiera con una unidad de CD-R puede copiar un programa de 400 dólares en un CD de un dólar. Cualquiera con una conexión a Internet medianamente rápida puede copiar cualquier cosa disponible en línea, en cualquier lugar del mundo, a su disco duro.

Bajo estas circunstancias, ejecutar la ley de derechos de autor contra los usuarios individuales es casi imposible. Si mi universidad decide ahorrar en su presupuesto de software comprando una copia de Microsoft Office y haciendo montones de copias, un empleado descontento con la dirección de correo electrónico de Bill Gates podría meternos en muchos problemas. Pero si elijo proporcionar copias a mi mujer e hijos (lo que no se me permite hacer según la licencia de Microsoft) o incluso a una docena de amigos, en la práctica hay poco que Microsoft pueda hacer al respecto.

Esto podría cambiarse. Si quisiéramos ejecutar la ley actual con el suficiente ahínco, podríamos. Todo ordenador del país sería sujeto a una búsqueda aleatoria. Cualquiera al que se le encontrara una copia

de software sin licencia iría directo a la cárcel. Silicon Valley se vaciaría y las prisiones se llenarían de frikis, adolescentes y niños.

Nadie lo considera una solución tolerable al problema. Aunque recientemente ha habido algún cambio en la dirección de la responsabilidad penal expandida por infringimiento de derechos de autor, las compañías de software en su mayor parte dan por hecho que no pueden usar la ley para evitar la copia individual de sus programas y, por tanto, han echado mano a otras maneras de beneficiarse de sus esfuerzos.

Los poseedores de derechos de autor musicales se enfrentan a problemas similares. A medida que la propiedad de grabadoras se fue volviendo común, la piratería se hizo más fácil. Cambiar temporalmente a los CD restauró el equilibrio, ya que proporcionaban una calidad superior a la cinta y eran caros de copiar, pero entonces llegaron los grabadores de CD baratos y el audio digital. Más recientemente, ya que las redes de ordenadores se han vuelto más rápidas, el almacenaje más barato y la compresión digital más eficiente, la amenaza ha venido de la distribución en línea de archivos MP3 con canciones sujetas a derechos de autor.

Enfrentados con la incapacidad de ejecutar la ley de derechos de autor contra los individuales, ¿qué deben hacer los poseedores de derechos de autor? Hay al menos tres respuestas.

1. Sustituir la protección tecnológica por la legal.

En los primeros días de los ordenadores domésticos, algunas compañías vendían sus programas en discos diseñados a prueba de copia. Los consumidores lo encontraron incómodo, bien porque querían hacer copias para sus amigos, bien porque querían hacer copias de seguridad para ellos mismos. Así que otras compañías de softwarevendieron programas diseñados para copiar los discos protegidos contra copias. Una compañía produjo un programa

(SuperUtility Plus) diseñado para hacer una amplia variedad de actividades útiles, incluyendo copiar los discos protegidos de otras compañías. Estaba hecho a prueba de copia. Así que otra compañía produjo un programa (SuperDuper) cuya única función en la vida era hacer copias de SuperUtility Plus.

La protección tecnológica continúa de muchas formas distintas. Todas se enfrentan a un problema común. Es bastante fácil proporcionar protección suficiente para evitar que el usuario medio emplee el software de maneras que no quiera el productor. Es muy difícil proporcionar protección adecuada contra un experto. Y una de esas cosas que los expertos pueden hacer es poner su maestría al servicio del usuario medio en forma de software diseñado para vencer los esquemas de protección.

Esto sugiere una posible solución: protección tecnológica apoyada por protección legal contra el software diseñado para vencerla. En los primeros años, los proveedores de protección anticopia probaron esa posición. Denunciaron a los fabricantes de software diseñado para romper la protección, argumentando que eran culpables de infringimiento contributivo (ayudar a otra gente a copiar material sujeto a derechos de autor), infringimiento directo (copiar y modificar el software de protección en el proceso de aprender cómo vencerlo) y violación de los términos de la licencia bajo la cual se vendía el software de protección. Perdieron[2].

Más recientemente, los poseedores de libertad intelectual apoyaron con éxito una nueva legislación (la Sección 1201 de la ley Digital Millennium Copyright Act [Ley de Ley de Derechos de Autor del Milenio Digital]) que revirtiera ese resultado, ilegalizando la producción o distribución de software cuyo objetivo principal sea saltarse la protección tecnológica. Queda por ver si esa restricción se podrá ejecutar.

---

[2] *Vault Corp. v. Quaid Software Ltd*, United States Court of Appeals, Fifth Circuit, 1988 847 F.2d 255, en http://cyber.law.harvard.edu/ilaw/Contract/vault.htm.

2. Controlar solo la copia a gran escala

Cualquiera con una grabadora de video, algo de software adicional y un poco de conocimiento puede copiar videos para sus amigos. Sin embargo, los videoclubes siguen funcionando. Proporcionan a sus clientes a un precio razonable una selección mayor que la que podrían obtener copiando las cintas de sus amigos. Las tiendas mismas no pueden violar la ley de derechos de autor de forma segura comprando una cinta por cada cien tiendas, porque son organizaciones grandes y visibles. Así que los productores de películas continúan obteniendo ingresos de las cintas a pesar de la habilidad de los clientes para copiarlas.

No hay una manera práctica de que las compañías musicales eviten que un adolescente haga copias de un CD o una colección de MP3 para sus amigos, pero los consumidores de música están dispuestos a pagar por una gama mucho más amplia de oportunidades disponible en una tienda. La razón por la que Napster amenazó a la industria musical fue que proporcionaba una gama similar de oportunidades a un precio mucho más bajo. La situación es similar en los programas de ordenador. Mientras que la ley de derechos de autor puede usarse para evitar la piratería a gran escala, los consumidores están dispuestos a pagar por la comodidad proporcionada por una fuente legal (por tanto, a gran escala y pública) para su software. En ambos casos, la habilidad de los propietarios de la propiedad intelectual para hacer la piratería lo suficientemente incómoda como para mantenerse en el negocio se ve amenazada por Internet, que ofrece la posibilidad de una distribución pública de música y software pirateados a gran escala.

3. Permitir la copia; conseguir beneficios de otras maneras.

La mayor parte de los ponentes de éxito te confiarán por lo bajo que no hay una actividad periodística o pedagógica más remunerativa, algo que apuntaron Mark Twain y Winston Churchill.

William F. Buckley, Jr[3]

Hace un siglo, los autores importantes ganaban gran parte de sus ingresos impartiendo conferencias públicas. A juzgar por la cita de Buckley (y mi propia experiencia), algunos todavía lo hacen, lo que sugiere que, en un mundo sin derechos de autor ejecutables, algunos autores podrían escribir libros, proporcionarlos en línea a cualquiera que los quiera y ganarse la vida vendiendo servicios a sus lectores (conferencias públicas, servicios de consultoría o similares). Esta no es una posibilidad puramente conjetural. Actualmente proporciono todo el texto de cuatro libros y numerosos artículos en mi página web, gratis, y recibo una amplia gama de beneficios, monetarios y no monetarios, haciéndolo.

Esto es un ejemplo de una estrategia más general: regala la propiedad intelectual y obtén beneficio indirectamente. Así es como se proporcionaban los dos navegadores web líderes. Netscape regaló Navigator y vendió el software del servidor con el que interactuaba Navigator; Microsoft siguió una estrategia similar. Apple proporcionó un navegador competitivo que estaba (y está) disponible de forma gratuita, pero solo funcionaba en los ordenadores Apple. Ahora mismo toda una variedad de navegadores son de código abierto, una solución crear software que discutiremos en el capítulo siguiente. También es como los programas de radio y televisión pagan las facturas; regalan el programa y consiguen ingresos de los anuncios.

Como muestran estos ejemplos, la muerte de los derechos de autor no significa la muerte de la propiedad intelectual. Sí significa que los productores de la propiedad intelectual deben encontrar otras formas

[3] Buckley, 2000, pp. xxii-xxiii.

de que se les pague por su trabajo. El primer paso es reconocer que, a largo plazo, limitarse a ejecutar la ley existente no va a ser una opción.

DIFAMACIÓN EN LÍNEA: UN EJEMPLO MENOS SIMPLE

Un periódico publica un artículo afirmando que soy un delincuente en busca y captura que ha sido la mente maestra detrás de varios ataques terroristas famosos. Los compañeros se sienten obligados a aceptar cuando les propongo salir a cenar. El jefe de departamento me asigna un curso los domingos por la mañana con solo un alumno. Comienzo a recibir llamadas anónimas. Mi recurso de acuerdo con la ley actual es demandar al periódico por difamación, obligándoles a retractarse de sus falsas afirmaciones y compensarme por el daño infligido.

Se dan por hecho dos cuestiones implícitas en la solución legal. Una es que cuando alguien realiza una falsa afirmación a la suficiente gente como para hacer un daño serio, la víctima puede bien identificar a la persona que realizó la afirmación, bien a otro responsable de que lo haya hecho (el periódico, si no el autor). La otra es que al menos una de las personas identificadas como responsables tendrán suficientes activos como para que merezca la pena demandar.

Hace veinte años, ambas suposiciones eran ciertas por lo general. El periodista que escribía un artículo difamatorio podía ser demasiado pobre para que mereciera la pena demandarlo, pero el periódico que lo publicaba no lo era, y sensatamente podría considerárselo responsable de lo que imprimía. Era posible difamar a alguien mediante el envío masivo de cartas anónimas, pero era demasiada complicación hacerlo en una escala lo bastante grande para que le importara a la mayor parte de las víctimas.

Ninguna de las dos es ya cierta. Es posible, con una ingenuidad mínima, conseguir acceso a Internet sin identificarte. Con un poco más de conocimiento técnico, es posible comunicarse en línea por medio de intermediarios (remitentes de correo anónimos) de una forma tal que el

mensaje no pueda ir ligado al emisor. Una vez en línea, hay maneras de comunicarse con un número elevado de gente casi a coste cero: correo electrónico masivo, publicaciones en noticias de Usenet, una página en la web. Y si se elige abandonar el anonimato y difundir mentiras con tu propio nombre, acceder a Internet es tan poco caro que está disponible fácilmente para la gente sin suficientes activos para que merezca la pena demandarlos.

Una respuesta posible es que debemos ejecutar la ley cueste lo que cueste. Si el que origina la difamación es anónimo o pobre, encuentra a otro, en alguna parte de la cadena de causalidad, que no sea ninguna de las doscosas. En la práctica, probablemente significa identificar el proveedor de servicios de Internet (ISP, en sus siglas inglesas) a través del que se transmitió el mensaje y tacharlo de responsable. Una página web está alojada en alguna máquina de algún sitio; alguien la posee. Un correo electrónico llegó en algún momento de un servidor de correo; alguien lo posee.

Esa solución no tiene más sentido que considerar responsable de las cartas anónimas a Correos. Es razonable esperar que el editor de un periódico sepa lo que aparece en sus páginas. Pero un ISP no tiene una manera práctica de vigilar el enorme flujo de información que circula por sus servidores, y, si pudiera, no querríamos que lo hiciera. Podemos (lo hacemos en el contexto de infringimiento de copyright) montar procedimientos bajo los que se pueda exigir a un ISP que desmantele material de la web. Pero eso no sirve de nada contra una publicación de Usenet, el correo electrónico masivo, la difamación web alojada en sitios reacios a ejecutar la ley estadounidense, o difamadores dispuestos a sufrir las molestias de alojar sus páginas web en múltiples servidores, cambiando de uno a otro si es necesario. La ley de la difamación tiene una utilidad muy limitada para evitar la difamación en línea.

Hay (siempre la ha habido) otra solución para el problema. Cuando la gente cuenta mentiras sobre mí, las respondo. Los desarrollos tecnológicos que convierten la ley de la difamación en inejecutable también posibilitan las magníficas herramientas para responder a las

mentiras y así proporcionar un sustituto, posiblemente superior, de la protección legal.

Mi ejemplo favorito es Usenet News, una parte de Internet más vieja y menos conocida que la Web. Para el usuario parece una colección de tablas de boletines en línea, cada una con un tema distinto: anarquía, radios de corta frecuencia, arquitectura, historia de la cocina. Cuando publico un mensaje en un grupo de noticias, el mensaje llega a un ordenador (un servidor de noticias) proporcionado por mi ISP. La próxima vez que el servidor de noticias hable a otro, intercambian mensajes y el mío se extiende gradualmente por el mundo. En una hora, podría responderlo alguien de Finlandia o Japón. El servidor que uso aloja más de cien mil grupos. Cada uno es una colección de conversaciones difundidas por el mundo, una diminuta comunidad no unida geográfica y, a menudo, dividida por intereses comunes.

Google, que aloja un popular motor de búsqueda web, también proporciona un motor de búsqueda para Usenet. Usándolo puedo descubrir en menos de un minuto si alguien ha mencionado mi nombre en cualquier parte del mundo en algún momento durante los últimos tres días (o semanas, o años) en uno de los más de cien mil grupos de noticias. Si obtengo un resultado, un click me muestra el mensaje. Si soy el David Friedman mencionado (el proceso sería más fácil si me llamara Myron Whirtzlburg) y si mi mensaje requiriera una respuesta, unos pocos clicks más ponen mi respuesta en el mismo hilo del mismo grupo de noticias, donde casi todos los que leyeron la publicación original lo verán. Es como si, cuando alguien me calumniara en cualquier parte del mundo, el viento me soplara sus palabras y llevara de vuelta mi respuesta a las orejas de todos los que las habían oído.

La protección que Usenet ofrece contra la difamación no es perfecta; una poca gente que leyó la publicación original podría perderse mi respuesta y más podrían elegir no creerla. Pero la protección ofrecida por los tribunales también es imperfecta. Las afirmaciones falsas más dañinas no son lo bastante importantes para justificar el coste y molestias de una demanda. Muchos de los que son responsables no

reúnen los requisitos legales de responsabilidad. Dada la opción, prefiero Usenet.

Supón que en vez de difamarme en un grupo de noticias lo haces en una página web. Es fácil encontrarlo: Google también proporciona un motor de búsqueda para la Web. El problema es cómo contestar. Puedo poner una página web con mi respuesta y esperar que lectores lo bastante interesados pasen por ella, pero eso es todo lo que puedo hacer. Los enlaces de tu página web los has puesto tú, no yo, y podrías ser reacio a añadir uno a la página que pruebe que estás mintiendo.

Hay una solución a este problema, una solución tecnológica. Los navegadores web actuales solo muestran enlaces directos, enlaces de la página a otras páginas. Sería posible construir un navegador web, llamémoslo Netscape Navigator 12.0, que mostrara automáticamente los enlaces de otras páginas a esta, permitiendo que el usuario no solo vea qué páginas eligió enlazar el autor de esta página a la suya, sino también qué páginas eligieron enlazarse a la suya[4]. Una vez sean de uso común esos navegadores, solo necesito subir una página con un enlace a la tuya. Cualquiera que muestre tu página con esta opción activada será conducido a mi refutación[5].

Hay un problema con esta solución: un problema legal. Tu página web está protegida por copyright, que te proporciona el derecho a prohibir que otra gente haga copias o trabajos derivados. Un navegador que muestra tu página como pretendías está haciendo una copia, pero un navegador al que has dado autorización explícita colgando tu página en la Web. Un navegador que muestre tu página con los enlaces que conectan a ella está creando un trabajo derivativo que podrías no haber pretendido y, como es razonable, no autorizaste. Para asegurarte de que

---

[4] Ya puedes obtener esa información usando Google para buscar páginas que enlacen a una página en particular. Esto es posible porque Google ya ha indexado toda la Web y, por tanto, tiene una lista completa de enlaces que pueden ser leídos por cualquiera de los lados. Un proyecto actual que sigue estas líneas es Crit, en http://zesty.ca/pubs/cscw-2002-crit.pdf.

[5] Un sistema así ya existe en una forma muy primitiva: el sistema *trackback* usado por los blogueros. Actualmente, los *trackbacks* son voluntarios por parte de los «enlazados a», pero si los navegadores sondearan ellos mismos los servidores *trackback*, podrían mostrar los enlaces en una barra lateral, sin necesitar ninguna acción por parte del sitio «enlazado a».

tus mentiras no se pueden responder, notificas a Netscape que no están autorizados a mostrar tu página añadiendo los vínculos hacia ella.

El tema de cuándo una página web es un trabajo derivativo no autorizado de otra se está gestando ahora mismo en el contexto de framing («encuadre»): un sitio web que presenta material de otro junto con su propia publicidad[6]. Si mi visión de la difamación en línea es correcta, el resultado de ese litigio podría ser importante para un conjunto de asuntos completamente distintos. La misma regla legal (una lectura férrea del derecho a evitar los trabajos derivativos en línea) que podría proteger un sitio de otra gente que esté usando su contenido también proporcionaría protección a alguien que quiere difundir mentiras en línea.

TERRENO PANTANOSO

Mi madre era una probeta, mi padre era un cuchillo.

Viernes, Robert A. Heinlein

Los cambios tecnológicos alteran el coste de hacer cosas. Pero también podrían afectarnos de una forma más sutil dejando obsoletas las categorías que empleamos para hablar y pensar el mundo que nos rodea.

---

[6] Este asunto se discute en http://www.templetons.com/brad/linkright.html y http://www.bitlaw.com/Internet/linking.html. Un desarrollo futuro que siga líneas similares (un servicio de noticias que utilice la información en la Web de otra gente para generar automáticamente noticias personalizadas para cada cliente) se discute en http://www.futurepundit.com/archives/002790.html y en http://writ.news.findlaw.com/hilden/20050524.html.

Piensa en la categoría de «padre». Lo normal era que, aunque pudiera haber algo de incertidumbre acerca de la identidad del padre del niño, no había duda acerca de qué significaban «padre» o «madre». Las leyes y normas sociales que especificaban los derechos y obligaciones de los padres y madres no eran ambiguas en su significado, si es que no eran siempre aplicables.

Ya no es el caso. Con la tecnología reproductiva actual, hay al menos dos significados biológicos de «madre» y pronto habrá un tercero. Una madre gestante es la mujer en cuyo útero se incuba un feto. Una madre ovular es la mujer cuyo óvulo fertilizado se convirtió en el feto. Una vez se convierta la clonación en una tecnología consolidada, una madre mitocondrial será la mujer cuyo óvulo, con su núcleo reemplazado por el núcleo del donante del clon pero con su propio ADN mitocondrial extranuclear, se desarrolló hasta convertirse en feto. Y una vez se convierta la ingeniería genética en una tecnología madura, permitiéndonos producir descendencia cuyo ADN sea un mosaico de múltiples donantes, el concepto de «una» madre biológica (o padre) no tendrá casi sentido.

El niño con cinco padres

Una pareja de California quería un hijo. El marido era estéril. La esposa era doblemente estéril: no podía producir un óvulo fértil ni llevar a término un feto. Celebraron un contrato con un donante de esperma, un donante de óvulo y una madre gestante. El óvulo donado se impregnó del esperma donado y se implantó en el útero alquilado. Entonces, antes de que naciera el bebé, el matrimonio se separó, dejando a los jueces con un rompecabezas: ¿Qué persona o personas tenían los derechos y obligaciones legales de paternidad?

Si se toma la ley de California al pie de la letra, la respuesta estaba clara. La madre era la mujer de cuyo cuerpo nacía el bebé. El padre era su marido. Era una normal legal lo bastante sensata cuando se

escribieron las leyes. Pero no tenía sentido alguno en un mundo donde ni aquella mujer ni su marido estaban relacionados con el bebé ni habían planeado ser sus padres.

El tribunal que al final decidió sobre el asunto sostuvo que los padres eran la pareja que había movido toda aquella cadena de acontecimientos al tener la intención por aquel entonces de criar al niño como si fuera suyo. Así sustituyeron una definición biológica que se había tornado tecnológicamente obsoleta por una definición social: una maternidad que venía dada no por los óvulos ni úteros, sino por la intención.

Esta es una historia real. Si no me crees, ve a una librería de Derecho y busca John A. B. v. Luanne H. H. (72 Cal. Rptr. 2d 280 [Ct. App. 1998]).

Los muertos vivientes

Pensemos en alguien cuyo cuerpo se encuentra preservado a la temperatura del nitrógeno líquido mientras espera el progreso médico necesario para revivirlo y curarlo. Legalmente está muerto; su esposa es viuda, sus herederos tienen su propiedad. Pero si se lo va a revivir realmente, en verdad no está muerto, sino meramente durmiendo muy profundamente. Nuestro sistema legal, más generalmente nuestra forma de pensar en la gente, no tiene en cuenta el estatus especial de dicha persona. Hay una categoría de vivo, una categoría de muerto y, fuera de los videojuegos y películas de miedo, nada entre ellas.

La ausencia de dicha categoría importa. Podría, literalmente, ser una cuestión de vida o muerte.

Estás muriendo de una enfermedad degenerativa que destruye gradualmente el cerebro. Si se te cura hoy, estarás bien. Si se te cura un año más tarde, tu cuerpo podría sobrevivir, pero no tu mente. Tras estudiar la situación, decides que estás más que dispuesto a cambiar un año de estar muriéndote por una oportunidad de recuperar la vida.

Llamas a la Fundación para la Extensión de la Vida Alcor y les pides que congelen tu cuerpo, a ser posible, mañana.

Contestan que, si bien están de acuerdo con tu decisión, no pueden ayudarte. Mientras estés vivo legalmente, congelarte es legalmente un asesinato. Simplemente tendrás que esperar otro año hasta que se te declare legalmente muerto y esperar que, de alguna manera, la ciencia médica sea capaz de reconstruirte de lo que quede para entonces.

Esta también es, permitiendo un poco de licencia poética, una historia real. En Donaldson v. Van de Kamp, Thomas Donaldson fue a juicio en un intento vano de conseguir permiso para congelarse antes de que, más pronto que tarde, un tumor cancerígeno destruyera su cerebro.

Los asuntos planteados por estos casos (el significado de la paternidad y la muerte) se discutirán con mayor amplitud en capítulos posteriores. Su función aquí es ilustrar la forma en que el cambio tecnológico altera el suelo conceptual bajo nosotros.

Todos nosotros nos las vemos con el mundo en términos de aproximaciones. Describimos a alguien como alto o bajo, amable o cruel, sabiendo que lo primero es una cuestión de grado y lo segundo, tanto de grado como de dimensiones múltiples. Pensamos que el parte meteorológico es cierto, aunque es bastante improbable que proporcione una descripción perfectamente ajustada del tiempo, o incluso que dicha descripción sea posible. Cuando el hombre del tiempo dice que la temperatura es de cuarenta grados a la sombra, ¿a qué centímetro cuadrado de la sombra se está refiriendo? Clasificamos una novela como ficción y este libro como no ficticio, aunque muchas de las afirmaciones de la primera sean ciertas y algunas de la última sean falsas.

Enfrentarnos al mundo de esta manera funciona porque el mundo no es un armazón aleatorio de objetos: hay un patrón. Las temperaturas varían de un trozo de sombra a otro, pero no por mucho. Aunque una afirmación sobre «la» temperatura en la sombra pueda no ser cierta de

forma precisa, raramente perdemos mucho al tratarla como si lo fuera. Casi lo mismo sucede con otras simplificaciones útiles de la realidad que hacen posible tanto el pensamiento como la comunicación.

Cuando el mundo cambia lo bastante, algunas simplificaciones dejan de ser útiles. Siempre fue cierto que había un continuo entre la vida y la muerte; el punto exacto en que a alguien se le declare legalmente muerto es arbitrario. Pero, con raras excepciones, era arbitrario por cuestión de segundos, quizás minutos, lo que casi nunca importaba. Pero cuando se sabe que, para mucha gente, la ambigüedad no solo existe, sino que existirá durante décadas, la simplificación ya no es útil. Podría, como pudo haber sucedido en el caso de Thomas Donaldson, convertirse en letal.

NO ES SOLO LA LEY, ES LA VIDA

Hasta ahora, mis ejemplos se han centrado en cómo las normas legales deberían responder al cambio tecnológico. Pero asuntos similares surgen para cada uno de nosotros viviendo nuestras propias vidas en un mundo cambiante. Piensa, para una historia en parte ya representada, en las relaciones entre hombres y mujeres.

El declive del matrimonio

Durante mucho tiempo, las sociedades humanas se han basado en variantes de la división sexual del trabajo. Todo comenzó con una coacción común: las mujeres dan a luz y amamantan al niño, los hombres, no. Para la sociedad de cazadores-recolectores, esto significaba que los hombres eran los cazadores y las mujeres, a las que se mantenía relativamente cerca del campamento por la necesidad de cuidar de los hijos, las recolectoras. En sociedades más civilizadas esto se convirtió, con muchas variaciones, en un patrón donde las mujeres

se especializaban en la producción del hogar y los hombres, en la producción externa al hogar.

Una segunda coacción era el deseo de los hombres de gastar sus recursos en sus propios hijos en vez de en los de otros, un deseo incluido en el hecho de que la selección de Darwin ha diseñado a los organismos, incluidos los machos humanos, para ser buenos transmitiendo sus propios genes a futuras generaciones. Dado que la única forma en que un hombre pueda estar razonablemente seguro de que es el padre de un niño particular era que la madre no hubiera tenido sexo con otros hombres durante el periodo en que se concibió, el arreglo usual de las sociedades humanas, con unas pocas excepciones, daba a los hombres exclusividad sexual. Un hombre podría, bajo algunas circunstancias, dormir con más de una mujer, pero se suponía que una mujer dormía con un solo hombre, y la mayor parte del tiempo lo hacía.

En los últimos siglos, dos circunstancias han alterado los hechos que llevaron a esas instituciones. Una fue el descenso en la mortalidad infantil. En un mundo donde tener dos o tres hijos adultos exigía que una mujer pasara la mayor parte de sus años fértiles embarazada y cuidando de los niños, la división sexual del trabajo era sólida: una profesión, «madre», absorbía casi la mitad de la fuerza productiva. En el mundo de hoy, una mujer solo necesita quedarse embarazada de dos bebés para acabar con dos hijos adultos.

Un segundo cambio, el incremento de la división del trabajo, ha reducido drásticamente la importancia de la producción en el hogar. Todavía se puede lavar la ropa, pero la mayor parte del trabajo la hace la gente que construyó la lavadora. Puede que todavía hagas la comida, pero es importable que cures el jamón o te hagas la sopa. Ese cambio eliminó gran parte de lo que hacían tradicionalmente las esposas, con lo que dejó libres a las mujeres para realizar otras actividades[7].

---

[7] “Let us accept the idea that women should stick to their own jobs – the jobs they did so well in the good old days before they started talking about votes

A medida que ser esposa y madre fue pasando de ser un trabajo de jornada completa a ser de tiempo parcial, las instituciones humanas se ajustaron. El empleo femenino en el mercado se amplió. El divorcio se volvió más común. La división sexual del trabajo, aun existiendo, es mucho menos pronunciada: muchas mujeres desempeñan trabajos que solían realizar casi exclusivamente los hombres, algunos hombres realizan trabajos que era costumbre que desempeñaran prácticamente en exclusivo las mujeres.

El futuro del matrimonio

Una consecuencia de que las mujeres casadas trabajen mucho fuera de casa es que hace que ejecutar la exclusividad sexual no sea nunca fácil[8], casi imposible. Las sociedades modernas desarrollaron una alternativa social: el matrimonio compañero. Es menos probable que una esposa que es tu mejor amiga en vez de tu subordinada o esclava quiera engañarte, algo bueno si no tienes una manera práctica de pararla. La sociedad moderna también produjo, algo más tarde, una alternativa tecnológica: el test de paternidad. Ahora es posible que un esposo sepa si los hijos de su mujer son suyos incluso si no está seguro de que él es su único compañero sexual.

---

and women's rights. . . . It is a formidable list of jobs: The whole of the spinning industry, the whole of the dying industry, the whole of the weaving industry. The whole catering industry and – what would not please Lady Astor, perhaps – the whole of the nation's brewing and distilling. All the preserving, pickling, and bottling industry, all the bacon-curing. And (since in those days a man was often absent from home for months together on war or business) a very large share in the management of landed estates. Here are the women's jobs. . . . "
Dorothy Sayers (1947, p. 133).

[8] Matthew Prior, "An English Padlock," es una argumentación en verso a favor del *companionate marriage* como solución a este problema. El poeta menciona todas las precauciones mediante las cuales un marido celoso puede intentar que su mujer se mantenga fiel y las maneras de que una mujer puede, si lo desea, vencer todas ellas, y saca como conclusión: «Let all her ways be unconfined/And clap your padlock on her mind» (Deja sus maneras fuera de la presa/Y coloca el candado en su cabeza).

Esto plantea algunas posibilidades interesantes. Podríamos tener (quizás estemos moviéndonos en esa dirección) una variante de las instituciones del matrimonio convencional en que las obligaciones paternales están determinadas por biología, no estado marital. Podríamos tener una sociedad con matrimonios en grupo pero con responsabilidades parentales individuales, ya que una mujer sabría cuál de sus múltiples maridos ha engendrado cualquier hijo en concreto. Podríamos tener una sociedad con sexo despreocupado pero obligaciones parentales bien definidas, aunque esto plantea ciertos problemas prácticos. Es mucho más fácil que una pareja comparta los deberes parentales si además están viviendo juntos, y el hecho de que dos personas disfruten durmiendo juntos es una prueba inadecuada de que vayan a disfrutar viviendo juntos.

Todos estos patrones de apareamiento ya existen (para una muestra parcial, métete en el grupo de noticias de Usenet alt.polyamory). Si se volverán comunes alguno de ellos dependerá en gran parte de la naturaleza de los celos sexuales masculinos. ¿Son primariamente un patrón aprendido, diseñado para satisfacer una preferencia instintiva por los hijos propios? ¿O es instintivo en sí mismo, programado por la evolución como una forma de mejorar las posibilidades de que los niños que mantiene un padre lleven sus genes?[9] Si se trata de lo primero, entonces una vez la existencia del test de paternidad vuelva obsoletos los celos, podemos esperar que sus manifestaciones desaparezcan, permitiendo una variedad de nuevos patrones de apareamiento. Si se trata de lo último, los celos seguirán siendo obsoletos, pero, dado el lento paso del cambio evolutivo, ese factor será irrelevante para el comportamiento durante mucho tiempo, por lo que podemos esperar seguir con alguna variante de la monogamia, o al menos poligamia consecutiva, como norma.

El principio básico aquí es el mismo que en ejemplos anteriores de ajuste al cambio tecnológico. Nuestro objetivo no es salvar el

---

[9] Me limito a los celos sexuales masculinos no porque los femeninos no existan, sino porque la tecnología relevante no ha cambiado: el conocimiento de una mujer de que un niño es suyo nunca ha dependido de saber si su padre se ha estado acostando con otras mujeres.

matrimonio. Es cumplir con los propósitos por cuyo cumplimiento evolucionó el matrimonio. Una forma es continuar con el viejo patrón incluso si se ha vuelto más difícil, como ejemplifica el movimiento de darle a las parejas la opción de un matrimonio de contrato, un matrimonio basado más en los viejos términos de «hasta que la muerte nos separe». Otra es aprovechar el avance tecnológico para cumplir el viejo objetivo (producir y criar niños) de nuevas maneras.

Hacer negocios en línea

La tecnología afecta a la ley y el amor. También al negocio. Piensa en el problema de la ejecución de los contratos.

Los litigios siempre han sido una manera patosa y de alto coste de ejecutar las obligaciones contractuales. Es posible demandar a alguien de otro estado federado, incluso de otro país, pero cuanto más distante sea la jurisdicción, más difícil es. Si el comercio en línea acaba por dispersarse no solo con la geografía sino con la identidad del mundo real, de forma que gran cantidad del comercio tenga lugar entre partes unidas solo por una identidad definida por una firma digital, ejecutar contratos en los tribunales se vuelve aún más difícil. Es complicado demandar a alguien si no sabes dónde está.

Hay una vieja solución: la reputación. Como en el caso de la difamación, la misma tecnología que hace los litigios menos prácticos hace al sustituto privado más práctico.

E-Bay proporciona un ejemplo de baja tecnología. Cuando ganas una subasta y recibes los bienes, se te da una oportunidad de informar del resultado (si el vendedor los entregó cuando y como estaba planeado, si los bienes estaban como se describieron). Los informes de todas las subastas pasadas de un cierto vendedor están disponibles, tanto en formato completo o resumido, para cualquiera que quiera pujar por las subastas presentes de este vendedor. En un capítulo subsiguiente evaluaremos mecanismos más elaborados, apropiados para

transacciones con mayores apuestas, por medio de las que la tecnología de la información moderna puede usar la ejecución basada en la reputación para sustituir la ejecución legal.

¿FRENOS? ¿QUÉ FRENOS?

Cuando evaluamos el inconveniente de las tecnologías (Asesinato Inc. en un mundo de privacidad férrea o un futuro villano de James Bond usando nanotecnología para reducir el mundo entero a pedazos), tu reacción podría ser «¡Para el tren, me quiero bajar!». En la mayor parte de los casos, no es una opción. Este tren en concreto no tiene frenos.

La mayor parte de las tecnologías que estamos discutiendo pueden desarrollarse localmente y usarse globalmente. Una vez que un país tenga una nanotecnología funcional, que le permita construir productos enormemente superiores a los que se hacían con las tecnologías antiguas, habrá una enorme presión para que los otros países sigan su ejemplo. Es difícil vender parabrisas de cristal cuando la competencia usa diamantes como estructura. Es todavía más difícil persuadir a los pacientes de cáncer de que estén satisfechos con la radioterapia cuando saben que, en otra parte del mundo, se encuentran disponibles máquinas de reparación de células microscópicas que simplemente van por el cuerpo y arreglan lo que esté mal. Para repetir un ejemplo ya dado, piensa en los contratos de madres de alquiler, acuerdos mediante los que una madre porta un hijo, sea de su óvulo o del de otra mujer, para que otra pareja lo críe como suyo. El caso Baby M estableció que dichos contratos no son ejecutables, al menos en Nueva Jersey. Lo siguiente fue la legislación de los estados federados, con el resultado de que en cuatro estados simplemente firmar un contrato de esta índole es un acto delictivo y que en uno, Michigan, preparar un contrato de madre de alquiler es un delito castigable con penas de hasta cinco años y cincuenta mil dólares.

Nada de esto importaba mucho. Alguien que pudiera permitirse los costes de contratar una madre de alquiler, y todavía más alguien que pudiera permitirse el coste necesario para que una madre incube el óvulo de otra, podría casi seguramente permitirse el coste adicional de hacerlo en un estado que lo permita. Siempre que haya uno que apruebe dichos arreglos, la desaprobación de otros tendrá poco efecto. E incluso si los contratos fueran inejecutables legalmente, solo sería cuestión de tiempo que la gente que estuviera en el negocio de prepararlos aprendiera a identificar y evitar a madres de alquiler potenciales que fueran susceptibles a cambiar de opinión una vez naciera el niño[10].

O piensa en la investigación sobre las causas del envejecimiento. Mucha gente cree (de forma equivocada, creo) que el mundo sufre serios problemas de sobrepoblación. Otros argumentan (de forma más razonable) que un mundo sin envejecimiento se expondría a la gerontocracia y el estatismo cultural. Muchos argumentarían (algunos lo hacen) que incluso si el problema del envejecimiento pudiera solucionarse, no debería hacerse.

Ese argumento se vuelve menos convincente cuanto mayor te vuelves. Los ancianos controlan grandes recursos, tanto económicos como políticos. Aunque los argumentos contra la investigación del envejecimiento podrían triunfar en alguna parte, es improbable que venzan en todas, y la cura solo tiene que encontrarse una vez.

Para dar un ejemplo más perturbador, pensemos en la inteligencia artificial, una tecnología que bien podría dejar obsoletos a los humanos. En cada estadio, hacerlo un poco mejor significa ser más capaz de diseñar productos, predecir movimientos bursátiles, ganar guerras. Esto casi garantiza que, en cada estadio, alguien vaya a dar el siguiente paso.

Incluso si es posible bloquear o restringir una tecnología potencialmente peligrosa, como podría ser en unos pocos casos, no está claro que debiéramos hacerlo. Podríamos descubrir que habíamos

---

[10] Silver, 1998, pp. 172–177.

perdido la enfermedad y prohibido la cura. Si un acuerdo internacional apoyado por una potencia militar aplastante tiene éxito en restringir el desarrollo nanotecnológico a laboratorios con la aprobación del Gobierno, esto podría salvarnos de la catástrofe. Pero como esos laboratorios son los que más probablemente estén trabajando en aplicaciones militares de nueva tecnología, mientras que los laboratorios privados intentan en su mayoría producir lo que quieren los clientes individuales, el efecto también podría ser evitar el desarrollo privado de medidas de respuesta nanotecnológicas a la destrucción masiva desarrollada por el Gobierno. O podría resultar que nuestras restricciones hubieran retardado el desarrollo de la nanotecnología lo bastante para dejarnos incapaces de defendernos frente al resultado de una tecnología diferente: una plaga genéticamente planeada, por ejemplo[11].

Hay argumentos legitimados para tratar de retardar o evitar algunos de estos desarrollos tecnológicos. Esas argumentaciones se realizarán[12], pero no aquí. Para mis fines, es más interesante dar por hecho que estos intentos, si se hacen, fracasarán, e intentar estudiar las consecuencias: cómo las nuevas tecnologías cambiarán las cosas, cómo los seres humanos se adaptarán a esos cambios y cómo deberían hacerlo.

El progreso tecnológico significa aprender más sobre cómo hacer cosas; frente a él, uno debería de esperar que acabe en una mejora de la vida humana. Hasta ahora, con pocas excepciones o ninguno, lo ha hecho. A pesar de una multitud de terribles predicciones durante los últimos dos años, la vida humana es hoy en día mejor en casi todas partes de lo que era hace cincuenta años, mejor cincuenta años atrás que hace cien años, y mejor cien que doscientos años[13].

---

[11] Para un retrato ficticio del problema, véase Sterling (1997) en http://www.cscs.umich.edu/~crshalizi/reviews/holy-fire/.

[12] Véase, por ejemplo, el ensayo de Bill Joy «Por qué el futuro no nos necesita» en http://www.oocities.org/es/loitaluddita/mencer/bill_joy.htm.

[13] Se ha discutido si la invención de la agricultura ha empeorado a la gente; la tecnología nueva podía sostener a una población mucho más densa, lo que tendía a desplazar a los cazadores-recolectores en competencia, pero lo hizo con un estilo de vida menos atractivo (Diamond, 1987, pp. 64–66) en http://www.ditext.com/diamond/mistake.html.

La experiencia pasada no siempre es un guía de confianza para el futuro. A pesar del progreso de los últimos doscientos años, mucha gente sigue prediciendo catástrofes futuras del progreso presente, incluyendo unos pocos lo bastante bien informados y competentes para que merezca la pena tomarlos en serio. En el último capítulo volveré a la cuestión de si, cómo y bajo qué circunstancias podrían tener razón.

SEGUNDA PARTE

PRIVACIDAD Y TECNOLOGÍA

TRES

UN MUNDO DE PRIVACIDAD FÉRREA

Ha habido mucha preocupación en los últimos años sobre el fin de la privacidad. Como veremos en los próximos dos capítulos, hay razón para estos miedos; el desarrollo de las tecnologías mejoradas para la vigilancia y el proceso de datos amenaza, por supuesto, nuestra capacidad para restringir el acceso de otra gente a información sobre nosotros. Pero una tercera tecnología, menos conocida, se encuentra trabajando precisamente en la dirección opuesta. Si los argumentos de este capítulo son correctos, pronto estaremos experimentando en parte de nuestras vidas (una parte cada vez más importante) un nivel de privacidad que los seres humanos jamás conocieron antes. Es un nivel de privacidad que no solo asusta al FBI y a la Agencia de Seguridad Nacional, dos organizaciones cuyo asunto rutinario consiste en entrometerse en los secretos de otra gente: a veces hasta me asusta a mí.

Comenzamos con un viejo problema: cómo comunicarnos con alguien sin que otra gente sepa lo que estamos diciendo. Hay una serie de soluciones familiares. Si estás preocupado por las escuchas, comprueba que nadie te escucha antes de decir cosas que no quieras que oigan los vecinos. Para estar aún más a salvo, mantén la conversación privada en medio de un gran campo abierto o un barco en medio de un lago. A los peces no les interesa y nadie más puede oírte.

Esta propuesta ya no funciona. Incluso en medio de un lago puede llegar el alcance de un micrófono de cañón. Los aleros no tienen por qué contener escuchas, solo un micrófono y un transmisor. Si te pones a buscar *bugs*, alguien todavía puede hacer rebotar un rayo láser contra tu ventana y usarlo para recoger la vibración de tu voz. No estoy seguro de si la observación por medio de satélite es aún lo bastante buena para leer labios desde la órbita, pero si no, pronto lo será. Gran parte de nuestra comunicación es ahora indirecta, mediante cables de teléfono, ondas aéreas, Internet. Las líneas telefónicas pueden pincharse, los mensajes del teléfono móvil o inalámbrico pueden interceptarse. Un

correo electrónico rebota a través de múltiples ordenadores de camino a su destino: cualquiera que controle uno de esos ordenadores puede, en principio, guardar una copia.

Para los mensajes escritos se utilizaba un conjunto diferente de viejas tecnologías. Una carta sellada con el anillo de sello del emisor no podía proteger el mensaje, pero, al menos, hacía saber al destinatario si se había abierto, a menos que el espía fuera muy bueno con un cuchillo caliente. Una carta mandada por medio de un mensajero de confianza era todavía más segura, siempre que mereciera la confianza.

Una solución más ingeniosa era proteger no el mensaje físico, sino la información que contenía codificando el mensaje y proporcionándole al receptor la fórmula para descifrarlo. Una versión simple era una clave de sustitución, en la que cada letra del mensaje original se reemplazara por una letra diferente. Si reemplazamos cada letra con la siguiente del alfabeto, obtenemos "btj" a partir de la palabra "así".

"Btj" no se parece mucho a "así", pero no es muy complicado, si tienes un mensaje largo y paciencia, deducir la sustitución y descifrar el mensaje. Esquemas de codificación más sofisticados recolocan las letras según una fórmula elaborada, o convierten letras en números y hacen aritmética complicada con ellas para convertir el mensaje (*plaintext*) en su versión codificada (*ciphertext*). Estos métodos se usaban, con grados de éxito variantes, en ambos bandos de la Segunda Guerra Mundial.

Había dos problemas con esta manera de guardar secretos. El primero, que era lento y difícil, llevaba gran cantidad de trabajo convertir un mensaje en su forma codificada o revertir el proceso. Valía la pena hacerlo si el mensaje era la orden que le decía a la flota cuándo y dónde atacar, pero no para conversaciones espontáneas entre gente normal.

Ese problema se ha solucionado. Los ordenadores que la mayoría de nosotros tenemos en nuestros escritorios pueden cifrar mensajes empleando métodos probablemente imposibles de resolver incluso para la Agencia de Seguridad Nacional, más rápido de lo que podemos escribirlos. Incluso pueden cifrar, y descifrar, la voz humana a medida que hablamos. La encriptación está ahora disponible no solo para el Estado Mayor Conjunto, sino para ti y para mí, para nuestra conversación normal.

El otro problema es que para leer mi mensaje cifrado necesitas la clave, la fórmula que describe cómo descifrarlo. Si no tengo una forma segura de mandarte mensajes, podría no tener tampoco una manera segura de mandarte la clave. Si te la mando por medio de un mensajero de confianza pero cometí un pequeño error sobre quién estaba autorizado a confiar en él, ahora otro tiene una copia y puede usarla para desencriptar mis futuros mensajes hacia ti. Esto podría no ser demasiado problemático para los Gobiernos, dispuestos a y capaces de enviar información de ida y vuelta en maletines enganchados con esposas a las muñecas de agregados militares, pero para los fines normales de gente normal no es una opción práctica.

Hace unos veinticinco años, este problema se resolvió. La solución era la encriptación en clave pública, una nueva manera de cifrar y descifrar mensajes que no necesita un canal de comunicación seguro para el mensaje ni la clave. El*software* para implementar esa solución está ahora disponible por todas partes.

La encriptación en clave pública funciona generando un par de claves (llamémoslas A y B), cada una de ellas un número largo que puede usarse para descifrar lo que la otra ha descifrado. Si encriptas un mensaje con A, alguien que posee solo A no puede descifrarlo, se necesita B. Si encriptas un mensaje con B, tienes que usar A para desencriptarlo. Si mandas a un amigo la clave A (tu clave pública) mientras que mantienes en secreto la clave B (tu clave privada), tu amigo puede usar A para encriptarte mensajes y puedes usar B para desencriptarlos. Si un espía consigue una copia de la clave A, también puede mandarte mensajes secretos, pero todavía no puede desencriptar los mensajes de tu amigo. Eso necesita la clave B, que nunca dejó de estar en tu posesión.

¿Cómo puede tener uno la información necesaria para encriptar un mensaje y, aun así, ser incapaz de desencriptarlo? ¿Cómo puede ser posible producir dos claves con la relación necesaria pero no, a partir de una clave, calcular la otra? La respuesta a ambas preguntas depende del hecho de que haya algunos procesos matemáticos mucho más fáciles de hacer en una dirección que en otra.

La mayor parte de nosotros puede multiplicar 293 por 751 razonablemente rápido, usando nada más sofisticado que lápiz y papel,

y obtener 220 043. Partir de 220 043 y encontrar la única pareja de números de tres dígitos que puede multiplicarse para obtenerlo requiere mucho más tiempo. La versión que más se usa de encriptación en clave pública depende de esa asimetría, entre multiplicar y factorizar, usando números mucho más grandes. Los lectores que todavía estén asombrados podrían estar interesados en echar un vistazo al Apéndice I de este capítulo, donde describo una forma muy simple de encriptación en clave pública conveniente para un mundo en que la gente sabe cómo multiplicar pero aún no ha aprendido a dividir, o comprobar una de las descripciones en línea de las matemáticas de los algoritmos de El-Gamal y RSA, las formas más comunes de encriptación en clave pública.

Cuando digo que la encriptación es indescifrable, lo que quiero decir es que no se puede descifrar con un coste razonable de tiempo y esfuerzo. Casi todos los esquemas de encriptación, incluyendo la encriptación en clave pública, se pueden descifrar con una cantidad ilimitada de tiempo. Si, por ejemplo, tienes la clave A y un mensaje de mil caracteres encriptado con ella, puedes desencriptar el mensaje haciendo que el ordenador cree todo mensaje de mil caracteres posible, encriptar cada uno con A y encontrar el que concuerde. De forma alternativa, si sabes que la clave B es un número de cien dígitos, podrías probar todos los números de cien dígitos posibles, uno tras otro, hasta que encuentres uno que desencripte un mensaje que has encriptado con la clave A.

Ambas opciones son lo que los criptógrafos describen como ataques de «fuerza bruta». Para implementar la primera, deberías comenzar haciéndote con una buena provisión de velas: el número de secuencias de mil caracteres posible es tan astronómicamente grande que, empleando el ordenador más rápido que ahora esté disponible, el Sol se habrá extinguido mucho antes de que termines. El segundo puede funcionar si la clave B es un número lo bastante corto, que es por lo que la gente que se toma en serio la violación de privacidad trata de aprobar leyes que restrinjan la longitud de las claves que emplea el *software* de encriptación.

LA ENCRIPTACIÓN ESCONDE…

Imagina que todo el mundo tiene una conexión a Internet y un *software* de encriptación adecuado, y que la clave pública de todo el mundo está disponible para el resto (publicado en la guía telefónica, digamos). ¿Qué sucede?

Lo que yo digo

Un resultado obvio es que puedo tener conversaciones privadas. Si quiero mandarte un mensaje que nadie más pueda leer, primero lo encripto con tu clave pública. Cuando respondes, encriptas tu mensaje con mi clave pública. El FBI, o mi vecino cotillo puede pinchar la línea: todo lo que obtiene es un galimatías para cualquiera que no tenga la correspondiente clave pública.

A quién

Incluso si el FBI no sabe lo que estoy diciendo, puede aprender mucho observando al que se lo digo (conocido en el intercambio como *análisis de tráfico*). Este problema también se puede resolver, usando la encriptación en clave pública y un *remailer* anónimo, un sitio de Internet que envía correos electrónicos. Cuando quiero comunicarme contigo, mando el mensaje al *remailer* junto con tu dirección de correo electrónico. El *remailer* te lo manda.

Si eso fuera todo lo que pasaba, alguien que pinchara la red podría rastrear el mensaje desde mí hasta el *remailer*y desde el *remailer* hasta ti. Para evitarlo, el mensaje al *remailer*, incluida tu dirección de correo electrónico, está encriptada con la clave pública del *remailer*. Cuando lo recibe, emplea su propia clave privada para desvestir la capa de encriptación, con lo que revela tu dirección, y manda el mensaje desencriptado. Nuestro espía hipotético ve cómo mil mensajes entran en el *remailer* y mil salen, pero no puede ni leer las direcciones de

correo de los mensajes que entran (están ocultos bajo una capa de encriptación) ni casan el mensaje que entra con el que sale.

¿Y si el *remailer* es una trampa, un soplón de quien me está espiando? Hay una solución simple. La dirección de correo a la que manda el mensaje no es la tuya, es la dirección de un segundo *remailer*. El mensaje que manda es tu mensaje más tu dirección de correo electrónico, todo ello encriptado con la clave pública del segundo *remailer*. Si estoy lo bastante paranoico, puedo hacer rebotar el mensaje a través de diez *remailers* diferentes antes de que te llegue. A menos que los diez estén trabajando para el mismo espía, no hay manera de que alguien pueda rastrear el mensaje de mí a ti. (Los lectores que quieran una descripción más detallada de cómo funcionan los *remailers* la encontrarán en el Apéndice II.)

Ahora tenemos una forma de correspondencia que es doblemente privada: nadie puede saber lo que estás diciendo y nadie puede descubrir a quién se lo dices. Pero todavía hay un problema.

Quién soy

Cuando interactuamos con otra gente, es útil ser capaz de demostrar tu identidad, lo que puede ser un problema en línea. Si estoy liderando una conspiración para derrocar a un Gobierno opresivo, quiero que mis compañeros conspiradores sean capaces de distinguir qué mensajes vienen de mí y cuáles de la policía secreta que se hace pasar por mí. Si estoy vendiendo servicios de consultoría en línea, necesito ser capaz de demostrar mi identidad para beneficiarme de la reputación labrada mediante proyectos de consultoría pasados y asegurarme de que nadie más se aproveche de dicha reputación haciéndose pasar por mí.

Ese problema también puede solucionarse mediante la encriptación en clave pública. Para firmar un mensaje digitalmente, lo encripto usando mi clave privada en vez de tu clave pública. Entonces te lo mando con una nota diciendo de quién es. Lo desencriptas con mi clave pública. El hecho de que lo que sale sea un mensaje y no un galimatías te dice que se encriptó con la clave privada concordante. Puesto que soy el único que tiene esa clave privada, el mensaje debe de ser mío.

Mi firma digital no solo demuestra que te mandé el mensaje firmado, lo hace de una forma de la que luego no puedo desentenderme. Si niego haberlo mandado, señalas que tienes una copia del mensaje encriptado con mi clave privada, algo que nadie salvo yo podría haber producido. Por tanto, una firma digital hace posible que la gente firme contratos a los que se les pueda atar, y lo hace de una manera mucho más difícil de falsificar que una firma ordinaria.

Y a quién pago

Si vas a hacer negocios en línea, necesitas una forma de pagar cosas. Los cheques y tarjetas de crédito dejan un rastro documental. Lo que queremos es una forma equivalente de moneda, una forma de realizar pagos que luego no pueden rastrearse, ni por ninguna de las partes ni por cualquier otro.

La solución, discutida en detalle en un capítulo posterior, es el dinero electrónico anónimo. Su característica esencial es que permite que la gente realice pagos mandando un mensaje, sin que ninguna de las partes tenga que saber la identidad del otro y sin que una tercera parte tenga que conocer la identidad de ninguno de ellos. Una de las muchas cosas para lo que puede usarse es pagar los servicios de un *remailer* anónimo, o una cadena de *remailers*anónimos, resolviendo así el problema de cómo meter a los *remailers* en el asunto sin sacrificar el anonimato de sus clientes. Otra, como veremos más tarde, va a ayudarnos a eliminar una de las principales molestias leves de la vida moderna: el *spam*.

Combina y agita

Combina la encriptación en clave pública, *remailers* anónimos, firmas digitales y el dinero electrónico y tenemos un mundo en que los individuales pueden hablar y comerciar con una seguridad razonable de que ninguna tercera parte los está observando.

Una consecuencia menos obvia es la capacidad de combinar el anonimato con la reputación. Puedes hacer negocios en línea sin revelar tu identidad del mundo real, tu verdadero nombre[14]. Demuestras que eres la misma persona que hizo negocios ayer, o el año pasado, firmando digitalmente los mensajes. Tu identidad en línea está definida por su clave pública. Cualquiera que quiera comunicarse contigo privadamente emplea esa clave para encriptar sus mensajes; cualquiera que quiera asegurarse de que eres la persona que mandó un mensaje la usa para comprobar tu firma digital.

Con la excepción del dinero electrónico completamente anónimo, todas estas tecnologías ya existen, implementadas en *software* que actualmente está disponible gratis. Ahora mismo, sin embargo, están limitadas en su mayoría al estrecho ancho de banda del correo electrónico (mandar mensajes de texto privados de un lado a otro). A medida que los ordenadores y las redes informáticas se vuelvan más rápidos, esto cambiará.

Viajé varios cientos de millas en dos ocasiones el mes pasado (una vez, en coche; otra, por aire) para dar una serie de charlas. Con solo pequeñas mejoras en la tecnología actual, podría haberlas dado desde mi oficina. Tanto la audiencia como yo habríamos estado llevando gafas de realidad virtual (gafas con las lentes reemplazadas por diminutas pantallas de ordenador). Mi ordenador estaría dibujando la visión de la sala de conferencias como se ve desde el escenario (incluyendo las caras de mi audiencia) a sesenta fotogramas por segundo. Cada persona de la audiencia tendría una visión similar, desde su sitio, dibujada por su ordenador. Los auriculares se encargan del sonido. El resultado sería la ilusión, para todos, de que estábamos presentes en la misma habitación viéndonos y oyéndonos.

La realidad virtual no solo disminuye los costes del viaje, también tiene otras ventajas. Algunas audiencias esperan un traje y corbata, y no solo no me gusta llevar corbatas, todas las que tengo poseen una

---

[14] El esbozo más temprano de estas ideas que he visto apareció en una historia de ciencia-ficción escrito por un científico informático: «True Names» [Verdaderos nombres], de Vernor Vinge (Vinge, 1987). El sentido del título era que, como en la fantasía tradicional, un hechicero debe proteger su verdadero nombre para evitar que otros usaran magia contra él, en un mundo en línea los individuos deben proteger sus identidades del mundo real para evitar que otros actuaran contra ellos en el espacio real.

atracción magnética hacia los artículos alimenticios con colores que contrastan. Para dar una conferencia en realidad virtual no necesito una corbata, ni siquiera una camisa. El ordenador puede añadir ambas a la imagen que manda por la red. También puede eliminar unas pocas arrugas, oscurecer el pelo y quitarme una década de mi edad aparente.

A medida que los ordenadores se vuelvan más rápidos, no solo pueden crear y transmitir mundos de realidad virtual, también pueden encriptarlos. Ello significa que cualquier interacción humana que solo tenga que ver con la vista y el sonido puede moverse al ciberespacio y protegerse mediante una privacidad férrea.

Entregando las llaves: una breve digresión

Para mandar un mensaje encriptado a un extraño o comprobar la firma digital en un mensaje de un extraño, necesito su clave pública. Un poco más arriba di por hecho que el problema desaparecería escribiendo la clave pública de todos en la guía telefónica. Aunque esta es una posible solución, no es muy buena.

Una clave publicada en la guía telefónica es solo tan digna de confianza como quien está publicando. Si nuestro malo hipotético puede hacer que su clave pública aparezca en la lista bajo mi nombre, puede leer mensajes destinados a mí y firmar mensajes falsos que provengan de mí con una firma digital que anule mi supuesta clave. Una guía telefónica es un sistema centralizado, vulnerable a fallos en el centro, sea por deshonestidad o incompetencia. Sin embargo, hay una solución simple descentralizada; como puedes adivinar, depende de la encriptación en clave pública.

Piensa en una organización conocida, como American Express, que la gente conoce y en la que confía. American Express se encarga de hacer que su clave pública sea muy pública (publicada en la ventana de cada oficina de American Express, impresa) y codificada magnéticamente, en toda tarjeta de crédito American Express, incluida en el margen de todo anuncio de American Express. Entonces entra en el negocio de la identidad.

Para aprovechar sus servicios, utilizo mi *software* para crear una pareja clave pública/clave privada. Entonces voy a una oficina American Express, llevando el pasaporte, carnet de conducir y la clave pública. Tras quedarse satisfechos con mi identidad, les entrego una copia de mi clave pública y ellos crean un mensaje diciendo, en un lenguaje que un ordenador pueda entender: «La clave pública de David D. Friedman, nacido el 2/12/45 y empleado de la Universidad de Santa Clara, es 10011011000110111001010110001101000...» Firman digitalmente el mensaje usando la clave privada de American Express, copian el mensaje firmado en un disco y me lo dan.

Para demostrar mi identidad a un extraño, le envío una copia del certificado digital de American Express. Ahora conoce mi clave pública, lo que le permite mandar mensajes encriptados que solo David Friedman puede leer y comprobar las firmas digitales para ver si son realmente de David Friedman. Alguien con una copia de mi certificado digital puede usarlo para demostrar a la gente cuál es mi clave pública, pero no pueden usarla para hacerse pasar por mí, porque no poseen la clave privada concordante.

De momento, este sistema tiene la misma vulnerabilidad que la guía telefónica; si American Express o uno de sus empleados están trabajando para el malo, pueden crear un certificado falso identificando la clave pública de otro como mía. Pero nada en un sistema de certificados digitales requiere confiar en una organización. Puedo mandarte por correo electrónico todo un paquete de certificados digitales —uno de American Express, uno de Correos, uno de la Iglesia Católica, uno de mi universidad, uno de Microsoft, uno de Apple, uno de Orange— y puedes hacer que tu ordenador compruebe todos ellos y asegurarte de que todos concuerdan. Es improbable que un solo malo se haya infiltrado en todos[15].

Hasta ahora he estado dando por hecho que las identidades del mundo real son únicas, que cada individuo tiene solo una. Pero todos nosotros tenemos, en un sentido muy real, múltiples identidades: cosas diferentes son identificadores relevantes para gente distinta. Lo que mis estudiantes necesitan saber es que un mensaje proviene de verdad del profesor que enseña el curso que estudian. Lo que mi hija necesita

---

[1515] http://www.pgp.com/.

saber es que realmente llegó de su padre. Uno puede imaginarse circunstancias donde sea importante mantener separadas múltiples identidades del mundo real, para esconder de alguna de las personas con las que interactúas características identificativas que quieras ser capaz de revelar a otras. Un sistema de autoridades certificativas múltiples hacen eso posible, siempre que recuerdes qué certificados enviar a qué receptor. Mandar a tu superior en una organización criminal en la que te estás infiltrando el certificado que te identifica como policía puede ser arriesgado.

UN MUNDO DE PRIVACIDAD FÉRREA

Una de las características atractivas del mundo creado por estas tecnologías es la expresión libre. Si me comunico en línea con mi propio nombre empleando la encriptación, solo me puede traicionar la persona con la que me estoy comunicando. Si lo hago usando una identidad en línea, con reputación pero sin conexión con mi identidad en el espacio real, ni siquiera la gente con la que me comunico puede traicionarme. Así, la privacidad férrea crea un mundo que es, de muchas formas, más seguro que aquel en el que vivimos ahora, un mundo donde puedes decir cosas con las que otra gente discrepa sin riesgo de castigo, legal o de otra forma.

Eso me lleva a otra digresión, una dirigida especialmente a mis amigos de derechas del espectro político.

La Segunda Enmienda virtual

La Segunda Enmienda de la Constitución estadounidense garantiza el derecho a llevar armas. Una interpretación plausible de su historia la ve como una solución a un problema de preocupación considerable para los pensadores del siglo XVIII: el problema de los ejércitos permanentes. Todos sabían que los ejércitos profesionales vencen a los aficionados. Todos sabían también —con la historia de la dictadura de

Cromwell todavía muy reciente— que un ejército profesional planteaba un serio problema de golpe de Estado militar.

La Segunda Enmienda representaba una solución ingeniosa a ese problema. Combina un pequeño ejército profesional bajo el control del Gobierno Federal con una milicia ciudadana enorme (todo hombre en edad adulta con capacidades físicas). Deja que el Gobierno Federal proporcione la suficiente estandarización para que las unidades milicianas de distintos estados federados puedan trabajar juntas, pero deja que los estados elijan a los oficiales, asegurándose así de que los estados y sus ciudadanos mantuvieran el control sobre la milicia. En caso de una invasión extranjera, la milicia proporcionaría una gran fuerza, si bien entrenada y disciplinada imperfectamente, para hacer de suplemento a un pequeño ejército normal. En caso de un intento de golpe del Gobierno Federal, el ejército federal se encontraría en desventaja de cien sobre uno.

La belleza de esta solución es que no depende de hacer ilegal un golpe militar, sino de hacerlo imposible. Para que suceda ese golpe, primero sería necesario desarmar la milicia. Pero hasta que el golpe ocurriera, la Segunda Enmienda evitaba que se desarmara a la milicia, puesto que un intento tal se vería como una violación de la Constitución y resistiría con fuerza.

Era una solución elegante hace doscientos años, pero soy menos optimista que algunos de mis amigos con respecto a su relevancia hoy en día. Los Estados Unidos tienen un ejército profesional mucho más grande respecto a su población del que tenían entonces; los estados federados son mucho menos independientes del Gobierno Federal de lo que era, y la distancia entre el armamento civil y militar ha incrementado enormemente.

También han cambiado otras cosas a lo largo de estos doscientos años. En un mundo basado ampliamente en la democracia y la televisión en red, es probable que los conflictos entre el Gobierno de EE.UU. y sus ciudadanos tengan que ver con la guerra de la información, no con las armas. Un Gobierno que quiera hacer cosas malas a sus ciudadanos las hará controlando el flujo de información para hacer que parezcan buenas cosas.

En ese mundo, una encriptación fuerte ampliamente disponible funciona como una Segunda Enmienda. Mientras exista, el Gobierno no puede controlar el flujo de información. Y una vez existe, eliminarla, como desarmar a una ciudadanía armada, es extraordinariamente difícil. Especialmente para un Gobierno que no puede controlar el flujo de información a sus ciudadanos sobre lo que está haciendo.

Si trabajas para Hacienda, detente aquí

La libertad de expresión es algo a favor de lo que está la mayoría de la gente, al menos en EE.UU. Pero una fuerte privacidad también reducirá el poder del Gobierno de formas obviamente menos deseables. Las actividades que ocurran enteramente en el ciberespacio serán invisibles para los de fuera, incluyendo a los que trabajan para el Gobierno Federal. Es difícil fijar impuestos o regular cosas que no puedes ver.

Si gano dinero vendiendo servicios en el ciberespacio y lo gasto en comprar bienes en el espacio real, el Gobierno puede fijar impuestos sobre mi gasto. Si gano dinero vendiendo bienes en el espacio real y lo gasto comprando servicios en el ciberespacio, pueden poner impuestos sobre mi renta. Pero si gano dinero en el ciberespacio y lo gasto en el ciberespacio, no pueden observar ni los ingresos ni el gasto, así que no tendrán nada para poner impuestos.

Algo similar sucede con la regulación. Actualmente soy un profesor universitario de Derecho, pero no un miembro del Colegio de Abogados de California, lo que hace ilegal que venda ciertos tipos de servicios legales en California. Supón que quisiera hacerlo de todas formas. Si lo hago como David D. Friedman, es probable que me meta en apuros. Pero si lo hago como Legal Eagle Online, cuidándome de mantener en secreto el verdadero nombre (la identidad del mundo real) de Legal Eagle, no hay mucho que el Colegio pueda hacer al respecto.

Para vender mis servicios legales, tengo que convencer a alguien para que los compre. No puedo hacerlo dirigiéndome a clientes potenciales de mis libros y artículos porque todos se publicaron con mi propio nombre. Lo que puedo hacer es empezar dando consejo gratis y, entonces, cuando los receptores descubran que el consejo es bueno

(quizás contrastándolo frente al consejo de sus abogados actuales), subir mi precio. Así, con el tiempo, me establezco una reputación legal para una identidad en línea garantizada por mi firma digital.

El consejo legal es un ejemplo; el argumento es general. Una vez esté bien establecida la privacidad férrea, la regulación gubernamental de servicios de información ya no podrá ejecutarse. Los Gobiernos podrían todavía intentar mantener la calidad de los servicios profesionales mediante profesionales certificadores, proporcionando información sobre quien creen que es competente. Pero ya no será posible obligar a los clientes a actuar sobre esa información, prohibirles legalmente que utilicen proveedores no certificados, como actualmente se les prohíbe legalmente emplear a abogados o médicos sin licencia que no han aprobado el Colegio.[16]

El lado negativo de la privacidad férrea

Reducir la capacidad del Gobierno para recaudar impuestos y regular las profesiones es, desde mi punto de vista, algo bueno, aunque algunos estarán de acuerdo. Pero también se aplica la misma lógica a las actividades del Gobierno que apoyo, como evitar robos y asesinatos. La privacidad en línea hará más difícil que la gente no comparta números de tarjetas de crédito robadas o información sobre cómo matar gente u organizar tramas para robar cosas o volarlas.

No es un gran cambio; Internet y la encriptación sólida simplemente hacen algo más fácil que los delincuentes hagan lo que ya están haciendo. Un problema más serio es que, posibilitando la combinación del anonimato y la reputación, una privacidad férrea hace posibles las compañías delictivas con reputación basada en la marca.

---

[16] Philip Zimmerman, creador del programa en clave pública PGP que se usa en todas partes, propuso e implementó una versión todavía más descentralizada: una web de confianza. Siempre que te mandas mensajes con alguien, te proporciona una lista de todas las claves públicas que conoce, así como las identidades de sus propietarios. Tu *software* guarda la información. Cuanta más gente te haya dicho que una clave pública particular pertenece a una persona en particular, más seguro estás de que es cierto. En efecto, todos se convierten en una autoridad certificatoria para los demás.

Supón que deseas que maten a alguien. El gran problema no es el coste; como puedes ver por informaciones públicas, contratar a un asesino a sueldo cuesta menos que comprar un coche, y la mayoría de nosotros podemos permitirnos un coche. El gran problema (dando por hecho que ya has resuelto cualquier escrúpulo moral) es encontrar un vendedor digno de confianza del servicio que quieres comprar. Ese problema, en un mundo de una fuerte encriptación distribuida por muchos sitios, lo podemos resolver. Piensa en mi plan de negocios para Asesinato Inc. en cuatro pasos:

1. Encarga carteles misteriosos en las autopistas principales. Cada una contiene un único número largo y el mensaje «escríbelo». Haz que aparezcan anuncios con el mismo mensaje en los periódicos principales.

2. Pon un anuncio de una página entera en el *New York Times*, aparentemente sin sentido.

3. Organiza un asesinato múltiple con objetivos ilustres, como estrellas de cine o figuras importantes del deporte. Quizás una bomba en los Óscar.

4. Manda un mensaje a todos los grandes medios diciéndoles que el número de todos esos carteles es una clave pública. Si la usan para desencriptar el anuncio del *New York Times*, obtendrán una descripción del asesinato, publicado el día antes de que sucediera.

Ahora tienes que asegurarte de que todo el mundo ha obtenido, o puede conseguir, tu clave pública, y que sabe que pertenece a una organización dispuesta a y capaz de matar gente. Una vez has tomado los pasos para decirle a la gente cómo publicar mensajes donde puedas leerlos, todo el mundo sabrá cómo mandarte mensajes que nadie más pueda leer y cómo identificar mensajes que solo puedan venir de ti. Ahora estás en el negocio de intermediario que vende los servicios de asesinos a sueldo. Los verdaderos asesinatos todavía tienen que tener lugar en el espacio real, así que ser un asesino a sueldo todavía tiene riesgos. Pero el problema de localizar un asesino a sueldo (cuando no participas con regularidad en mercados ilegales) se ha solucionado.

Asesinato Inc. es un ejemplo particularmente dramático del problema de las empresas criminales con reputación basada en marca, que operan abiertamente en el ciberespacio mientras mantienen en secreto su

identidad y localización en el espacio real, pero hay muchos otros. Piensa en «Intercambio de Secretos Inc. Compra y Venta». O en un archivo pirata en línea que venda la propiedad intelectual de otros en formato digital, programas informáticos, música y mucho más, por un céntimo por euro que se puede pagar en dinero digital anónimo.

Con posibilidades tan poco atractivas, es tentador deducir que la única solución es prohibir la encriptación. Una propuesta más interesante es encontrar maneras de conseguir nuestros objetivos (evitar el asesinato, proporcionar incentivos para producir programas informáticos) que se hagan más sencillos por los mismos cambios tecnológicos que hacen más difíciles las viejas formas.

El anonimato es la defensa definitiva. Ni siquiera Asesinato Inc. puede asesinarte si no saben quién eres. Si planeas hacer cosas que podrían hacer que la gente te quiera matar (publicar un libro burlándote del profeta Mahoma, digamos, o revelar los verdaderos delitos de Bill (Gates o Clinton), sería prudente no hacerlo con un nombre ligado a tu identidad en el espacio real. Esa no es una solución completa (el que contrata el asesino a sueldo podría, después de todo, ser tu mujer, y es difícil vivir un matrimonio completamente en el ciberespacio), pero al menos protege a muchas víctimas potenciales.

Algo similar para el problema más común, si bien menos grave, de proteger la propiedad intelectual en línea. La ley del *copyright* se volverá inejecutable, pero hay otras maneras de proteger la propiedad. Una (usar la encriptación para proporcionar el equivalente digital de una alambrada que protege tu propiedad) la discutiremos por extenso en el capítulo 8.

Por qué no se detendrá

Durante las últimas dos décadas, elementos poderosos del Gobierno de EE.UU., sobre todo la Agencia de Seguridad Nacional y el FBI, han estado argumentando a favor de las restricciones sobre la encriptación diseñadas para mantener su habilidad para pinchar teléfonos, leer registros confiscados, y violar la privacidad de toda una variedad de formas por lo que consideran buenos propósitos. Tras mi descripción

del lado negativo de la privacidad férrea, los lectores podrían pensar que hay mucho que decir a favor de la idea.

Sin embargo, hay problemas prácticos. El más serio es que el pastel ya está descubierto: lo ha estado más de veinticinco años. Los principios matemáticos sobre los que se basa la encriptación en clave pública son de conocimiento público. Esto significa que un programador informático competente con interés en el tema puede escribir *software* de encriptación. Mucho de este *software* ya se ha escrito y está disponible a nivel global. Y, dada la naturaleza del *software*, una vez tienes un programa, puedes hacer un número ilimitado de copias. Se sigue que mantener el *software* de encriptación fuera del alcance de espías, terroristas y delincuentes con competencia no es una opción práctica. Probablemente ya lo tienen, y si no, pueden hacerse con él fácilmente.

Prohibir la producción y posesión de *software* de encriptamiento no es una opción práctica, pero ¿y prohibir o restringir su uso? Para ejecutar una ley de prohibición de esa índole las agencias ejecutoras vigilarían aleatoriamente una fracción sustancial de todas las comunicaciones, aprovechándose de la capacidad masiva de pinchar teléfonos que la actual ley exige que les proporcionen las compañías telefónicas y expandiendo los requisitos legales para aplicarlos también a otros proveedores de comunicaciones. Cualquier mensaje que sonara a chino y no pudiera mostrar que es el resultado de una forma legal de encriptación llevaría a acción legal contra su autor.

Un problema práctico es el enorme volumen de información que fluye por las redes informáticas. Un segundo problema es que, mientras que es lo bastante fácil decir si un mensaje consta de texto escrito en castellano, es mucho más difícil (en la práctica, imposible) identificar otro tipo de contenidos lo bastante bien como para estar seguro de que no consisten, o no contienen, mensajes encriptados.

Piensa en una foto digital de tres millones de píxeles. Está hecha de tres millones de puntos coloreados, cada uno descrito por tres números (intensidad de rojo, intensidad de azul, intensidad de verde)[17]. Cada

[17] http://www.sjgames.com/SS/. Según las historias de las noticias de 2007, en 2005 el juez supremo del Tribunal de Vigilancia de Inteligencia Extranjera (FISA) se quejó al Departamento de Justicia de que el FBI había suministrado repetidamente al tribunal información inadecuada para conseguir órdenes de vigilancia: «Los registros muestran que el

uno de estos números es, desde el punto de vista del ordenador, una cadena de unos y ceros. Cambiar el dígito de más a la derecha (la «parte menos significativa») de uno a cero o de cero a uno tendrá solo un diminuto efecto en la apariencia del punto, así como cambiar el dígito más a la derecha en un número decimal largo, digamos 9 319 413, tiene solo un efecto muy pequeño en su tamaño.

Para ocultar un mensaje encriptado de un millón de caracteres en mi foto digital, sencillamente reemplazo la parte menos significativa de cada uno de los números en la foto por una parte del mensaje. La foto es ahora una imagen marginalmente peor de lo que era, pero no hay manera de que un agente del FBI, o un ordenador que trabaje para el FBI, pueda saber de forma precisa cómo debería ser la foto. Es un ejemplo simple de *esteganografía*: ocultar mensajes.

No es práctico que la ejecución de la ley evite que los delincuentes sofisticados, espías o terroristas posean y usen un *software* de encriptación sólido. Lo que es posible es poner límites al *software* de encriptación públicamente comercializado y usado (insistir, por ejemplo, en que si AOL o Microsoft construyen una encriptación en sus programas, esta debe contener una puerta trasera que permita leer el mensaje sin la clave a las personas debidamente autorizadas, digamos, un agente de la ley con una orden judicial).

El problema con esta propuesta es que no hay manera de darle a la ejecución legal lo que quiere sin imponer costes muy altos al resto de nosotros. Para lidiar con los delitos que se están desarrollando, la policía tiene que ser capaz de descodificar información que han obtenido razonablemente rápido; sirve de poco leer el mensaje interceptado una hora después de que la bomba haya estallado[18]. El equivalente en el espacio real serían las reglas legales que permiten que los agentes de la ley abran cualquier cerradura del país en media

---

Tribunal de la FISA aprueba casi toda solicitud de órdenes, lo que da a los agentes amplios poderes para vigilarfísica y electrónicamente a la gente que, alegan, está conectada con casos de espionaje o terrorismo. El número de peticiones ascendió de 886 en 1999 a 2074 en 2005. El tribunal no rechazó ni una sola petición en 2005, pero "modificó" 61, según un informe del Departamento de Justicia para el Congreso». Fuente: http://www.washingtonpost.com/wpdyn/content/article/2007/03/26/AR2007032602073 pf.html.

[18] Este pasaje se escribió por primera vez antes del ataque del 11 de septiembre al World Trade Center. Este suceso fortaleció la mano de los que apoyaban la regulación de la encriptación, pero creo que la predicción a largo plazo todavía se sostiene.

hora. Esto no solo incluye la cerradura de tu puerta, sino las que protegen cámaras de los bancos, secretos de comercio, registros de abogados, listas de contribuidores a causas no populares y mucho más.

Mientras que el acceso estaría limitado nominalmente a aquellos autorizados debidamente, es difícil imaginar un sistema lo bastante flexible como para cumplir la tearea pero que no sea vulnerable a un mal uso. Si ser un policía te da acceso a cerraduras con millones de dólares tras ellas, en metálico, diamantes o información, algunos policías se convertirán en delincuentes y algunos delincuentes, en policías. Una autorización como es debida seguramente significa una orden judicial, pero no todos los jueces son honestos, y media hora no es suficiente para que ni siquiera un juez honesto verifique lo que el policía que solicita la orden le dice.

La encriptación proporciona las cerraduras para el ciberespacio. Si nadie tiene una encriptación fuerte, todo lo del ciberespacio es vulnerable ante un delincuente privado lo bastante sofisticado. Si la gente tiene una encriptación fuerte pero viene con una puerta trasera obligatoria accesible en media hora a cualquier policía con una orden judicial, entonces todo lo del ciberespacio es vulnerable a un delincuente privado con los contactos adecuados. Esas cerraduras tienen material que vale miles de millones de dólares tras ellas: dinero en los bancos, secretos comerciales en los ordenadores.

Uno podría imaginar un sistema para acceder a los documentos encriptados tan riguroso que necesitara permiso escrito del presidente del Gobierno, del Tribunal Supremo y el fiscal general y que solo se usara cada dos o tres años. Un sistema así no perjudicaría seriamente las operaciones en línea. Pero tampoco serviría realmente para ejecutar la ley, ya que no habría forma de saber qué comunicación de los miles de millones que se entrecruzan por Internet cada día necesitan descifrar.

Para que las regulaciones sean útiles, tienen que o evitar el uso rutinario de la encriptación o hacer razonablemente fácil que los agentes de la ley accedan a mensajes encriptados. Hacer cualquiera de las dos perjudicará seriamente el uso ordinario de la red. No solo dañará las transacciones rutinarias, hará más fácil el delito informático al restringir la tecnología más apropiada para defender contra él. Y lo

que conseguimos a cambio es protección, no contra el uso de terroristas y delincuentes sofisticados de la encriptación (no hay forma de evitar eso), sino solo contra el uso de gente ordinaria y criminales no sofisticados.

Los lectores que han leído la lógica del argumento podrían señalar que incluso si no podemos evitar que los delincuentes sofisticados usen una encriptación fuerte, podríamos ser capaces de evitar que la gente ordinaria lo use para tratar con delincuentes sofisticados, y hacer eso haría inviable mi plan de negocios para Asesinato Inc. Mientras que sería una pena dañar seriamente el desarrollo del comercio en línea, algunos podrían pensar que merece la pena pagar el precio para evitar las consecuencias indeseables de una privacidad férrea.

Para explicar por qué no espero que pase necesito una breve digresión económica.

Derechos de propiedad y miopía

Estás pensando en entrar en el negocio de plantar árboles: madera noble que madure lentamente pero produzca madera de valor. Desde que se plante hasta que se recoja se necesitan cuarenta años. ¿Debería hacerlo? La respuesta obvia es que no, a menos que estés seguro de que vivirás al menos otros cuarenta años.

Como muchas respuestas obvias, es errónea. De aquí a veinte años serás capaz de vender la tierra, cubierta de árboles de veinte años, por un precio que refleje lo que aquellos árboles valdrán en otros veinte años. Siguiendo la lógica, es sencillo mostrar que si por lo que esperas vender los árboles hará más que recuperar tu inversión, incluyendo cuarenta años de interés compuesto, deberías hacerlo.

Esto da por hecho un mundo de derechos de propiedad seguros. Supón que, en lugar de ello, damos por hecho que es bastante probable que, en algún punto de los próximos cuarenta años, robarán los árboles, sea legalmente por medio de una confiscación del Gobierno o ilegalmente por alguien que conduzca hasta el bosque por la noche, los corte y se los lleve. En ese caso solo estarás dispuesto a meterte en el negocio de la madera noble si lo que recibes por vender los árboles es lo

bastante superior a la recuperación normal de las inversiones para compensarte por el riesgo.

Generalizando el argumento, podemos ver que la planificación a largo plazo depende de derechos de propiedad seguros. Si confías en que lo que posees hoy todavía lo poseerás mañana (a menos que elijas venderlo), puedes permitirte renunciar a los beneficios de hoy a cambio de mayores beneficios mañana, o el año que viene, o la próxima década. Cuanto mayor sea el riesgo de que te quiten lo que poseas ahora en algún momento del futuro, mayor ha de ser el incentivo para limitarte a proyectos a corto plazo.

Los políticos de una sociedad democrática tienen derechos de propiedad inseguros sobre sus activos políticos; Bill Clinton podría alquilar la Casa Blanca, pero no podría venderla. Una consecuencia es que en un sistema así la política gubernamental está dominada por las consideraciones a largo plazo —más comúnmente, el efecto de la política actual en los resultados de las próximas elecciones—. Muy pocos políticos aceptarán costes políticos hoy a cambio de beneficios dentro de diez o veinte o treinta años, porque saben que cuando los beneficios lleguen, los disfrutará otro que esté en el poder.

Evitar el desarrollo de una privacidad de hierro significa dañar intensamente el crecimiento actual del comercio en línea. Significa hacer más fácil que los delincuentes se metan en nuestros ordenadores, intercepten mensajes, defrauden a bancos, roben tarjetas de crédito. Así, es probable que resulte costoso políticamente, no dentro de diez o veinte años, sino en el futuro inmediato.

¿Qué obtenemos a cambio? El beneficio de regular la encriptación (el único beneficio sustancial, ya que no podemos evitar que los criminales competentes usen la encriptación) es prevenir el crecimiento de una fuerte privacidad. Desde el punto de vista de los Gobiernos y de la gente que se encuentre en posición de controlarlos, podría ser un gran beneficio, ya que dicha privacidad amenaza con reducir seriamente el poder del Gobierno, incluido el poder de recaudar impuestos. Pero esta es una amenaza a largo plazo, que no se volverá seria hasta dentro de una o dos décadas. Vencerla requiere que la generación presente de políticos elegidos haga cosas que sean costosas políticamente para ellos.

Todo para proteger el poder de quienes sea que ocupen sus cargos en diez o veinte años.

Las políticas de regular la encriptación hasta ahora concuerdan con las predicciones de este análisis. El apoyo a la regulación ha provenido casi en su totalidad de burocracias de vida longeva como el FBI y la Agencia de Seguridad Nacional. Hasta ahora, al menos, han sido incapaces de conseguir que los políticos elegidos hagan lo que ellos quieran cuando tiene algún coste político serio.

Si este argumento es cierto, es improbable que la regulación seria de la encriptación, suficiente para hacer las cosas mucho más fáciles para la ejecución de la ley y mucho más difícil para el resto de nosotros, llegue a existir, al menos en los Estados Unidos. Así que hay una posibilidad razonable de que acabemos con algo que siga las líneas del mundo de la privacidad de hierro que hemos descrito en este capítulo.

Desde mi punto de vista, es bueno. La atracción de un ciberespacio protegido por la encriptación es que es un mundo en que todas las transacciones son voluntarias: no puedes recibir una bala a través de una línea T1. Es un mundo donde la tecnología defensiva ha vencido por fin a la ofensiva. En el mundo en que ahora vivimos, nuestros derechos se pueden violar por la fuerza o por fraude; en un ciberespacio protegido por una privacidad blindada, solo mediante el fraude. El fraude es peligroso, pero menos que la fuerza. Cuando alguien te ofrece un trato demasiado bueno para ser verdad, puedes rechazarlo. La fuerza hace posible ofrecer ofertas que no puedes rechazar.

Verdad para contar

En varias partes de este capítulo he simplificado los mecanismos de encriptación, describiendo cómo algo se podía hacer pero no cómo se hace. Así, por ejemplo, la encriptación en clave pública generalmente se realiza no mediante encriptación del mensaje con la clave pública del receptor, sino con la encriptación del mensaje con un esquema anticuado de encriptación con clave única, encriptando la clave única con la clave pública del receptor, y mandando tanto el mensaje encriptado como la clave encriptada. El receptor utiliza su clave privada

para desencriptar la clave encriptada y la usa para desencriptar el mensaje. Aunque esto es un poco más complicado que el método que he descrito, en el que el mensaje mismo está encriptado con la clave pública, también es significativamente más rápido.

De forma similar, una firma digital se calcula usando una función *hash* unidireccional para crear un resumen del mensaje original y encriptando dicho resumen con tu clave privada, para después mandar el mensaje y el resumen. El receptor desencripta el resumen, crea un segundo resumen del mensaje usando la misma función *hash*, y los compara para asegurarse de que son idénticos, como serán si el mensaje no se ha cambiado y concuerden las claves públicas y privadas.

Tales complicaciones hacen más difícil describir la mecánica de la encriptación y son casi completamente irrelevantes para los asuntos discutidos aquí, así que las he ignorado.

Un segundo conjunto de complicaciones, también ignorado pero más importante, concierne a las maneras indirectas en que el anonimato protegido criptográficamente podría resultar atacado. Un ejemplo es el análisis textual. Un lector perspicaz o un *software* lo bastante sofisticado podría reconocer las similitudes estilísticas entre los libros de David Friedman y el consejo legal escrito de Legal Eagle. Las posibilidades de que la misma persona haya leído trabajos de ambas identidades lo bastante atentamente para identificarlas como del mismo autor podría no ser muy alta, pero un *software* diseñado para análisis textual podría crear una base de datos que relacionara a un número muy grande de autores conocidos con los identificadores estilísticos de su escritura. Uno simple en mi caso sería usar demasiado "de ahí".

Otro problema es que la mayor parte de lo que he descrito depende de que tengas un control total sobre tu ordenador, o, al menos, sobre una pequeña tarjeta que contenga tu clave privada y el *software* suficiente para usarla para encriptar y desencriptar. Si otro puede obtener tu tarjeta privada mediante una intrusión, física o virtual, todo puede pasar. Si otro se puede hacer con el control de tu ordenador, incluso sin acceder a tu clave privada, puede usar ese control para engañarte de varias formas (por ejemplo, informando falsamente de que un mensaje tiene una firma digital válida). Como dice Mark Miller, «La gente no

firma, los ordenadores firman». Y encriptan, desencriptan y comprueban firmas. Así que un elemento crucial de la privacidad férrea es la capacidad de los individuos para controlar los ordenadores que usan. En la práctica, es probable que un sistema seguro incluya previsiones para cancelar públicamente las claves privadas que puedan haber caído en las manos equivocadas.

Una alternativa es memorizar tu clave privada. Una clave de 128 bits puede representarse como una cadena de diecinueve números, letras y signos de puntuación, lo que no es tan difícil de memorizar. Si no, la clave puede derivarse de una contraseña, un procedimiento que es menos seguro pero más sencillo para el usuario. En cualquier caso, todavía tienes el problema de asegurarte de que puedes confiar en que tu ordenador olvide la clave en cuanto la haya usado.

CUATRO

PROCESAMIENTO DE INFORMACIÓN: ¿AMENAZA O INTIMIDACIÓN? O

SI LA INFORMACIÓN ES PROPIEDAD, ¿QUIÉN LA POSEE?

Hace algunos años decidí montar mi propio sitio web. Una cuestión que se me planteó era qué cantidad de mi vida quería incluir. ¿Quería que alguien que buscara mi trabajo académico (quizás un empresario potencial) descubriera que invertía mucho tiempo y energía en investigar las recetas medievales, un tema que no tiene relación con el derecho ni la economía, probando así (de forma discutible) que era un diletante más que un académico serio? ¿Quería que algún empresario potencial descubriera que tenía opiniones políticas que no están de moda, que abarcan desde el apoyo a la legalización de las drogas hasta el apoyo a la inmigración abierta? ¿Y quería que alguien que podría indignarse por mis ideas políticas fuera capaz de descubrir cómo somos los miembros de mi familia y dónde vivimos?

Llegué a la conclusión de que mantener mi vida en compartimentos separados no era una opción práctica. Podría haber montado sitios separados para cada parte, sin conexión entre ellos, pero alguien con algo de iniciativa podría haber encontrado todos ellos con un motor de búsqueda. E incluso sin un sitio web, cualquiera que quisiera saber sobre mí podía encontrar vastas cantidades de información mediante una búsqueda rápida de Usenet, donde he contribuido activamente desde hace más de quince años. Mantener callada mi boca virtual no era un precio que estuviera dispuesto a pagar, y no valía nada menos que eso.

Este no es un problema nuevo. Antes de que existiera Internet, todavía tenía que decidir hasta qué punto quería vivir en mundos múltiples; si,

por ejemplo, debería discutir mis aficiones o ideas políticas con mis compañeros de trabajo. Lo que ha cambiado es la escala del problema. En un mundo enorme donde la información personal seextendía, sobre todo, por medio del cotilleo y se procesaba casi por completo por los cerebros humanos individuales, los hechos acerca de mí se encontraban, hasta un punto considerable, bajo mi control, no porque fueran secretos, sino porque nadie tenía el tiempo y la energía para descubrir todo lo que se podía conocer sobre los demás. A menos que fuera una gran celebridad, yo era el único especializado en mí.

Esto no era cierto en todas partes. En los buenos, viejos tiempos (digamos, los últimos tres mil años), una razón para huir a la gran ciudad era hacerse con un poco de privacidad. En los pueblos en los que la mayor parte del mundo vivía, los asuntos de cualquiera eran los asuntos de todos. En Sumeria, o Roma, o Londres los muros no eran más opacos y no eras menos visible que en casa, pero pasaban tantas cosas, tanta gente, que nadie podía seguirlo todo.

Esa forma de privacidad (privacidad por oscuridad) no puede sobrevivir al procesamiento de datos moderno. Ningún individual puede seguir el rastro de todo, pero muchos de nosotros tenemos máquinas que pueden. Los datos de una vida individual no son notablemente más complicados de lo que eran hace dos mil años. Es cierto que el número de vidas se ha incrementado por treinta o cuarenta en los últimos dos mil años, pero nuestra capacidad para manejar datos ha aumentado mucho más que eso. No solo podemos seguir el rastro de los datos personales de una sola ciudad: podemos, al menos limitadamente, guardar constancia de los datos del mundo entero, dando por hecho que los tuviéramos y quisiéramos.

Las implicaciones de estas tecnologías se han vuelto cada vez más visibles durante los últimos diez o veinte años. Muchas son altamente deseables. La capacidad de reunir y procesar vastas cantidades de información permite actividades humanas que antes habrían sido imposibles; hasta cierto punto, acaba con las constricciones de la geografía sobre la interacción humana. Pensemos en dos ejemplos.

Hace treinta y algo años, pasé varios veranos como consejero en un campamento para niños superdotados. Muchos de los niños, y algunos de mis compañeros, se hicieron amigos míos, solo para desaparecer al

final del verano. De vez en cuando me preguntaba qué habría sido de ellos.

No puedo parar de preguntármelo, al menos por algunos. Unos pocos años atrás, alguien que había estado en el campamento organizó una lista de correo para los antiguos participantes del campamento y los consejeros; los miembros son ahora más de doscientos. Esa lista existe por las tecnologías que hicieron posible no solo la comunicación sencilla con gente dispersa por todo el país, sino también encontrarlos en primer lugar: buscar en un pajar muy grande unos pocos centenares de agujas. Echando un vistazo a una página de Yahoo! Groups, encuentro casi tres mil de esas listas, cada una para un campo diferente; la más grande tiene más de setecientos miembros.

Para mi segundo ejemplo, piensa en un grupo de noticias Usenet Newsgroup con el que me encontré hace muchos años, dedicado a una consola tecnológicamente ingeniosa pero ya obsoleta desde hace mucho, de la cual tuve dos unidades: una para mi hijo y otra para mí. Leyendo las publicaciones, descubrí que alguien del grupo había localizado a Smith Engineering / Western Technologies, la compañía que tenía el *copyright* de Vectrex y sus juegos, y escribió para pedir permiso para hacer copias de los cartuchos de juego. La respuesta, claramente de la persona que diseñó la máquina, fue un sí entusiasmado. Obviamente estaba encantado de descubrir que todavía había gente jugando con su juguete, su sueño, su bebé. No solo aprobaba copiar cartuchos, si alguien quería escribir nuevos juegos, estaría contento de proporcionar el *software* necesario. Fue un ejemplo llamativo, para mí reconfortante, de la capacidad de la tecnología de comunicaciones moderna de unir a la gente con entusiasmos compartidos.

Vectrex tenía trucos cuando todavía se conocían como fallos — de un Preguntas Frecuentes, de Gregg Woodcock

EL MERCADO DE LA INFORMACIÓN

Mis ejemplos hasta ahora son pequeños y no comerciales: gente que sabe los secretos de otra gente o que se reúne con viejos amigos o

extraños con intereses comunes. Mientras que tales aplicaciones de la tecnología de la información son una característica cada vez más importante en el mundo en que vivimos, no son para nada tan destacadas o políticamente conflictivas como los usos comerciales a larga escala de la información personal. Un primer paso para comprender estas actividades es pensar en por qué alguna gente podría querer recopilar y usar información individual sobre un gran número de desconocidos. Piensa en dos ejemplos.

Planeas abrir una nueva tienda de ultramarinos en una cadena existente: un riesgo comercial de millones de dólares. El conocimiento de la gente que vive en el vecindario, lo probable que sea que compren en tu tienda y cuánto, es crucial. ¿Cómo lo obtienes?

El primer paso es descubrir qué tipo de gente compra en las tiendas que tienes ya y el qué. Para hacerlo, ofreces a los clientes una tarjeta de compra. La tarjeta se usa para obtener descuentos, de forma que los compradores pasen la tarjeta por un lector casi cada vez que pasen por caja, con lo que te proporcionan muchísima información detallada sobre sus patrones de compra. Una forma de emplear esa información es mejorar el diseño de las tiendas existentes; si la gente que compra macarrones casi siempre compra la salsa al mismo tiempo, ponerlos en el mismo pasillo hará más cómoda la tienda, por tanto más atractiva, por tanto más rentable.

Otra forma es ayudarte a decidir dónde colocar tu nueva tienda. Si descubres que la gente mayor como media no compra mucho de lo que vendes, quizás una comunidad de jubilados es el lugar erróneo. Si las parejas con hijos jóvenes hacen todas sus compras los fines de semana cuando un progenitor se puede quedar en casa con los niños, los solteros compran tras el trabajo de los días laborales (los fines de semana son para fiestas) y la gente jubilada a lo largo del día laboral (colas más cortas), entonces una localización con una mezcla adecuada de los tres tipos te dará un flujo de clientes más igualado, una mayor utilización de la tienda y mayores beneficios. Combinando la información de tus clientes con información acerca de la demografía de localizaciones alternativas, que el censo de EE.UU. proporciona gratuitamente o las empresas privadas a un precio superior, puedes mejorar sustancialmente las posibilidades de tu apuesta.

Para una aplicación tecnológica superior de la informática, piensa en la publicidad. Cuando leo una revista, veo los mismos anuncios que los demás, en su mayoría cosas que no me interesan. Pero una página web puede mandar una respuesta diferente para cada pregunta, personalizando los anuncios que veo para que sean de mi interés. Ningún anuncio televisivo, puesto que no tengo televisión, muchos anuncios de dispositivos de alta tecnología.

Para mostrarme los anuncios correctos, la gente que gestiona la página necesita saber en lo que estoy interesado. La sorprendente prueba de que esa información se encuentra ya allí y está usándose aparece en mi buzón de forma regular: una tonelada de catálogos.

¿Cómo me identificaron las compañías que mandan esos catálogos como cliente potencial? Si pudieran verme, sería sencillo. No solo llevo un brazalete que me identifica como tecnófilo (Casio lo llama reloj databank), llevo el modelo que, además de proporcionar una calculadora, base de datos y un calendario para compromisos, también se ajusta tres veces al día con el reloj atómico de EE.UU. para asegurarse de que tiene la hora correcta. Las empresas Sharper Image, Techno-Scout, Innovations y demás no pueden ver lo que tengo en la muñeca, aunque si la sociedad transparente del siguiente capítulo llega a tener lugar, esto podría cambiar. Sin embargo, pueden hablar las unas con las otras. Cuando compré mi Casio Wave Captor Databank 150 (el nombre habría sido más largo, pero se quedaron sin espacio en el reloj), esa adquisición proporcionó información sobre mí a los propietarios del catálogo del que lo compré. Sin duda vendieron esa información a cualquiera que estuviera dispuesto a pagar por ella. Los vendedores de dispositivos respondieron a la adquisición de un Casio Wave Captor de la manera en que los tiburones responden a la sangre en el agua.

A medida que nuestra tecnología mejora, se vuelve posible crear y usar información de esta índole a un precio más bajo y con mucho más detalle. Una página web puede rastrear no solo lo que compras, sino también lo que miras y durante cuánto. Combinando información de muchas fuentes, se vuelve tanto posible como potencialmente rentable crear bases de datos con información detallada sobre el comportamiento de un número muy elevado de individuos, sin duda incluyéndome, probablemente incluyéndote.

Las ventajas de esa tecnología para los clientes individuales son muy obvias. Si voy a ver anuncios, preferiría que fueran de cosas que podría querer comprar. Si se me va a interrumpir mi cena por una llamada de teléfono de un desconocido, preferiría que fuera de alguien que me ofrece podar mi anciano albaricoquero (la recolección del año pasado fue una gran decepción) más que alguien que me ofrece refinanciar mi hipoteca inexistente.

Como sugieren estos ejemplos, que la información personal se encuentra disponible públicamente y sea fácil de encontrar reporta ventajas a los individuos. ¿Qué desventajas hay? ¿Por qué hay tanta gente enfadada por la pérdida de privacidad y el mal uso de «su» información privada? ¿Por qué Lotus, tras anunciar su plan de ofrecer toneladas de esa información en un CD, tuvo que cancelarlo en respuesta al masivo criticismo público? ¿Por qué se plantea la pregunta de qué información se permite que los sitios web recopilen sobre sus clientes, qué pueden hacer con ella y qué deben decir a sus clientes sobre lo que van a hacer con ella, un asunto legal y político vivo?

Una respuesta sentimental es que mucha gente siente de forma intensa que esa información sobre ellos es suya. Deberían ser capaces de decidir quién la consigue; si va a venderse, ellos deberían recibir el dinero.

La respuesta del economista es que ya reciben el dinero. El hecho de que venderme un dispositivo proporcione al vendedor una información que puede volver a vender luego hace la transacción un poco más rentable para el vendedor, atrae a vendedores adicionales, y, en última instancia, reduce el precio que debo pagar por el dispositivo. El efecto es diminuto, pero también lo es el precio que podría obtener por la información si, de alguna forma, dispusiera la venta yo mismo. Solo es la suma de grandes cantidades de dicha información lo que es lo bastante valioso para que merezca la pena la molestia de comprarla y venderla.

Una respuesta diferente, motivada por la intuición moral más que por la economía, es que el argumento confunde la información sobre mí (localizada en la base de datos o la mente de otro) con la información que me pertenece. ¿Cómo puedo tener un derecho de propiedad sobre los contenidos de tu mente? Si soy tacaño o mentiroso, ¿tengo el

derecho inherente a prohibir a los que trato mal pasar esa información? Si no, ¿por qué debería tener el derecho de prohibirles pasar otra información sobre mí?

Sin embargo, hay una razón más vaga, pero más importante, por la que la gente se molesta por la idea de un mundo donde cualquiera dispuesto a pagar pueda aprender casi todo sobre ellos. Mucha gente valora su privacidad no porque quieran ser capaces de vender información sobre ellos, sino porque no quieren que otra gente la tenga. Mientras que es difícil que se nos ocurra una explicación clara de por qué nos sentimos así (un tema discutido por extenso en el capítulo final de esta sección), está claro lo que hacemos. En cierto nivel, el control sobre la información sobre nosotros se ve como una forma de autoprotección. Cuanta menos gente pueda saber de mí, menos probable es que utilicen esa información sobre mí para dañarme o identificarme como alguien a quien deseen dañar. Lo que nos lleva de vuelta a alguno de los asuntos que he estudiado cuando montaba mi página web.

Hacia la información como propiedad

Las preocupaciones respecto a la privacidad se aplican al menos a dos tipos de información personal. Una es la información generada por transacciones voluntarias con otra parte: qué productos he comprado y vendido, a qué catálogos y revistas me he suscrito, qué páginas web visito. Esta información comienza en la posesión de ambas partes de la transacción: sé qué te he comprado, sabes lo que me has vendido. El otro tipo es la información generada por acciones que realizo que son públicamente visibles: registros judiciales, historias de periódicos, cotilleo.

La posesión del primer tipo de información puede, al menos en principio, determinarse por contrato. Una revista puede, y algunas lo hacen, prometer a sus suscriptores que no se venderán sus nombres. Las empresas de *software* ofrecen por rutina a la gente que se registra en sus programas la opción de que sus nombres estén o no disponibles para otras empresas que vendan productos similares. Las páginas web

pueden, y muchas lo hacen, proporcionar políticas de privacidad explícitas que limitan lo que harán con la información generada en el proceso de entrar en sus sitios.

Para comprender la economía del proceso, piensa en la información como un bien producido; como otros bienes así, quién posee cuánto viene determinado por el acuerdo entre las partes que la producen. Cuando me suscribo a una revista, el editor y yo estamos produciendo conjuntamente una información sobre mis gustos: la información de que me gusta ese tipo de revista. Esa información es de valor para la revista y podría querer revenderla. Es de valor para mí, o porque podría querer revenderla o porque podría querer mantenerla fuera del mercado para proteger mi privacidad. El editor puede, vendiendo suscripciones a un precio menor sin una garantía de privacidad que con, ofrecer pagarme por el control de la información. Si la información vale para mí más que lo que está ofreciéndome, me niego; si vale menos, acepto. El control sobre la información acaba con quien más la valora. Si no se pueden encontrar términos mutuamente aceptables, no acepto y esa información no se produce.

Esto parece implicar que las normas predeterminadas sobre la privacidad, normas que especifican quién comienza poseyendo la información, no debería importar. Eso sería cierto en un mundo en que preparar contratos fuera gratis, un mundo con cero costes de transacción. En el mundo en que vivimos ahora, no lo es. La mayoría de nosotros, a menos que nos importe mucho nuestra privacidad, no nos molestamos en leer políticas de privacidad. Incluso si prefiero que los catálogos y listas de correo no revendan información sobre mí, es demasiada molestia comprobar la letra pequeña de todo a lo que me suscriba. Sería todavía más molestia si toda firma con la que haya tratado ofreciera dos precios, una con y otra sin garantía de privacidad, y todavía más si la firma ofreciera un menú de niveles de protección, cada uno con su precio asociado.

El resultado es que la mayoría de las revistas y sitios web, al menos según mi experiencia, ofrecen un conjunto único de términos; si permiten alguna elección al suscriptor, no está ligada al precio, probablemente porque las cantidades sean demasiado pequeñas para que merezca la pena regatear. De ahí que las normas predeterminadas

importen y que tengamos conflictos políticos y legales acerca de la pregunta de quién, fuera de cualquier acuerdo contractual explícito, tiene qué control sobre la información personal generada por transacciones.

Esto podría cambiar. Lo que podría cambiarlo es la tecnología: la tecnología de agentes inteligentes. En principio es posible, y se está volviendo posible en la práctica, programar nuestro navegador web con información sobre tus preferencias de privacidad. Usando esa información, el navegador puede decidir qué niveles distintos de protección de la privacidad te valen o no y seleccionar según esto páginas y términos. Los navegadores trabajan barato.

Para que suceda, necesitamos un lenguaje de privacidad, una manera en que una página web pueda especificar qué hace o qué no hace con la información generada por tus interacciones con ella de forma que el navegador pueda comprenderlo. Una vez exista tal lenguaje y se use globalmente, los costes de transacción de regatear sobre la privacidad sufrirán un profundo descenso. Le dices a tu navegador lo que quieres y lo que vale para ti, tu navegador interactúa con un programa en el servidor web que aloja la página y que configura el dueño de la página. Entre ellos acuerdan los términos que satisfagan a ambos, o no lo consiguen y nunca ves la página.

Esta no es una idea puramente hipotética. Su encarnación actual es la Plataforma a favor de las Preferencias de Privacidad (P3P), apoyada por varios de los navegadores web líderes. Las páginas web proporcionan información sobre sus políticas de privacidad, los usuarios proporcionan información sobre lo que están dispuestos a aceptar, y el navegador notifica al usuario si las políticas de un sitio son incoherentes con sus requerimientos. Presumiblemente, un sitio web que representa mal sus políticas podría ser considerado responsable por hacerlo, aunque, que yo sepa, ningún caso así ha llegado todavía a los tribunales.

Cómo no proteger la privacidad

Seguro contar un secreto a uno,
Arriesgado a dos,
Contarlo a tres es una locura,
Todos lo sabrán.

Hávamál,
siglo IX

Supón que resolvemos los problemas de los costes de la transacción, con lo que permitimos un verdadero mercado de la información personal. Ahí sigue quedando un segundo problema: ejecutar los derechos por los que has firmado. Puedes comprobar los contenidos de tu cuenta para asegurarte de que todavía están ahí, pero no sirve para nada comprobar los contenidos de una base de datos de una firma para asegurarte de que tu información todavía está ahí. Pueden vender tu información y todavía tenerla.

El problema de ejecutar los derechos con respecto a la información no se limita a un mundo futuro de contratos automatizados: existe hoy en día. Como me gusta plantearlo cuando discuto la ley de privacidad actual, solo hay dos maneras de controlar la información sobre ti y una de ellas no funciona.

La forma que no funciona es dejar que otra gente tenga información sobre ti y entonces crear normas sobre cómo usarla. Esta es la propuesta de la ley de privacidad moderna. Si estás en desacuerdo con mi evaluación, sugiero un simple experimento. Comienza con cinco mil dólares, el nombre de un vecino aleatorio y busca en las páginas amarillas «Investigadores». El objetivo es acabar con un informe de crédito sobre tu vecino, algo que, según la Ley Federal de Reporte sobre el Crédito Justo, no se te permite tener. Si eres un estafador competente o un gurú de Internet, probablemente puedes prescindir del dinero y el listín telefónico.

Esta propuesta de proteger la privacidad funciona mal cuando se ejecutan los términos impuestos por la ley federal. Debería funcionar algo mejor para ejecutar términos que se han acordado en el mercado,

ya que, en ese caso, se apoya por sanciones reputacionales, así como legales: las empresas no quieren ganarse la reputación de engañar a sus clientes. Pero todavía no esperaría que funcionara excelentemente. Una vez que la información esté ahí, es muy difícil seguir el rastro de quién la tiene y lo que ha hecho con ella. Es particularmente difícil cuando hay muchos usos de la información que no quieres evitar: un problema central con la Ley de Reporte de Crédito Justo. Montar las normas que permiten que solo la gente con una razón legítima para mirar a tu informe de crédito es difícil: ejecutarlas lo es más.

La otra forma de proteger la información, la que sí funciona, es no dejar que salga la información en primer lugar. Así es como la privacidad férrea del anterior capítulo se protegía. No tienes que confiar en que tu proveedor de servicios de Internet o en el operador de un *remailer* anónimo no cuente tus secretos; no les has dado ningún secreto que puedan contar.

Hay problemas con la aplicación de esta propuesta a la información transaccional. Cuando te suscribes a una revista, el editor sabe quién eres, o, al menos, dónde vives: necesita esa información para que te llegue la revista. Cuando me compras algo, sé que te lo he vendido. La información comienza en la posesión de ambos: a falta de amnesia controlada, ¿cómo puede acabar solo en la posesión de uno?

En nuestro mundo presente, ese es un problema casi insuperable. Pero en un mundo de privacidad férrea, no tienes que saber a quién se lo estás vendiendo. Si, en algún punto del futuro, la privacidad es lo suficientemente importante para la gente, las transacciones en línea se pueden estructurar para hacer que cada parte sea anónima para la otra, con envíos en línea por medio de un *remailer* (para transacciones de información) o mediante el espacio real, menos cómodo, equivalente a un sistema de envío físico. Si no te he revelado la información, no la tienes, así que no necesito preocuparme sobre lo que vas a hacer con ella.

Volviendo a algo más parecido a nuestro mundo presente, uno puede imaginar instituciones que permitirían un grado considerablemente mayor de control individual sobre los usos de la información personal que ahora existe, modeladas según acuerdos usados ahora para mantener el control de las empresas sobre sus listas de correo valiosas.

Los individuos que se suscriban a una revista mandarían al vendedor no su nombre y dirección, sino el nombre del intermediario de información que han contratado y el número mediante el cual el intermediario los identificó. El editor de la revista mandaría al intermediario cuatro mil copias y los números que identifican a los cuatro mil suscriptores (anónimos), el intermediario pondría las etiquetas de las direcciones y las mandaría por correo. La información nunca abandonaría las manos del intermediario, una empresa del negocio de proteger la privacidad. Para comprobar su honestidad, establezco una identidad con mi propia dirección y el nombre «David Freidmann», me suscribo a una revista usando esa identidad y veo si David Freidmann recibe algún correo basura.

Estas instituciones serían posibles y, si se usaran globalmente, no extremadamente caras. Mi suposición es que nunca tendrán lugar. La razón es que la mayoría de la gente o no quiere mantener en secreto la información relevante (yo no, por ejemplo; me gustan los catálogos de dispositivos tecnológicos) o no lo quieren lo bastante como para pasar por cualquier molestia significativa. Pero todavía merece la pena pensar en cómo podrían obtener privacidad si quisieran, y esos pensamientos podrían volverse de una relevancia más práctica si el progreso tecnológico reduce ampliamente el coste.

DOS CAMINOS HACIA LA PROPIEDAD DE LA INFORMACIÓN PERSONAL

Estas discusiones sugieren dos formas distintas en que las tecnologías que ayudan a crear el problema podrían usarse para resolverlo. Ambas son formas de hacer posible que un individuo trate la información sobre sí mismo como de su propiedad. Una va a usar tecnologías informáticas, incluida la encriptación, para darme a mí o a mis agentes de confianza un control directo sobre la información, permitiendo que otros la usen solo con mi permiso (por ejemplo, para mandarme información sobre bienes que piensan que podría querer comprar) sin nunca poseerla. La otra es tratar la información como ahora tratamos a los bienes raíces: permitir a los individuos poner restricciones sobre el

uso de la propiedad que poseen que aten a los adquiridores posteriores. Si, por ejemplo, te vendo una servidumbre que te permita cruzar mi tierra para llegar a la tuya y después vendo la tierra, la servidumbre sirve contra el comprador. Incluso si no sabía que existía, ahora no tiene derecho a negarse a dejarte pasar.

Esto no es así en la mayoría de las otras formas de propiedad[19]. Si te vendo un coche con la restricción de que estés de acuerdo en que no se permita que se conduzca los domingos, podría ser capaz de ejecutar esa restricción contra ti; podría ser capaz de denunciarte por daños si, en contra del contrato, lo vendes a otro sin exigirle que se ciña al acuerdo. Pero no tengo manera de ejecutar la restricción sobre esa otra persona.

Una explicación plausible de la diferencia es que la propiedad de la tierra involucra un sistema elaborado para registrar el derecho, incluidas las modificaciones como servidumbres, con lo que posibilita que el posible comprador determine con antelación qué obligaciones van con la tierra. No tenemos un sistema así para registrar la propiedad, mucho menos para registrar formas complicadas de propiedad, para la mayor parte de los otros tipos de propiedad.

A primera vista, la información personal parece incluso menos apropiada para la forma más elaborada de los derechos de propiedad que los bolígrafos, mesas u ordenadores. En la mayoría de los usos probables, el adquisidor está comprando información sobre un número muy elevado de gente. Si mi información particular solo vale tres céntimos, un régimen legal que le exija gastar un dólar comprobando las restricciones sobre ella antes de que la use significa que la información nunca se usará.

Una solución posible es aprovecharse de las mismas tecnologías de procesamiento de datos que hacen posible juntar y usar información en esa escala para mantener el registro de los derechos de propiedad complicados sobre ella. Uno podría imaginar un régimen legal en que toda información personal tuviera que acompañarse de un número de identificación único. Usando ese número, un ordenador podría acceder a la información sobre las restricciones sobre el uso de esa

[19] Una excepción es que las demandas contra la propiedad usada como fianza para un préstamo podrían extenderse a la propiedad (y lo hacen, en el caso de los automóviles, donde dichas demandas normalmente se registran en el documento título).

información en un formato que pueda leer una máquina a un coste insignificante. De nuevo, no parece probable en el futuro cercano, pero podría convertirse en una posibilidad real más adelante.

CINCO

TECNOLOGÍA DE VIGILANCIA

El panóptico universal

La tendencia empezó en Gran Bretaña hace una década, en la ciudad de King's Lynn, donde sesenta videocámaras por control remoto se instalaron para escudriñar los conocidos como «puntos problemáticos», informando directamente a la comisaría. La reducción de los delitos callejeros resultante excedió todas las predicciones; en o cerca de las zonas bajo vigilancia, descendió a una decimoséptima parte de la cantidad anterior. Solo el ahorro en los costes de patrulla pagó el equipamiento en unos pocos meses. Docenas de ciudades y pueblos pronto siguieron el ejemplo de King's Lynn. Glasgow, Escocia, informó de un 68% de bajada en los delitos de la ciudad, mientras que la policía de Newcastle denunció a más de mil quinientos autores de delitos con pruebas grabadas (todos salvo siete se declararon culpables, y aquellos siete fueron condenados después). En mayo de 1997, mil hinchas de fútbol del Newcastle arrasaron las calles del centro. Los detectives que estudiaron las cámaras eligieron ciento cincuenta y dos caras y publicaron ochenta fotos en los periódicos locales. A los días, todos fueron identificados.

David Brin, The Transparent Society, capítulo 1, p. 5 [Traducción nuestra].

A principios del siglo XIX, Jeremy Bentham, uno de los pensadores ingleses más curiosos y el más original, diseñó una prisión en que todo prisionero pudiera ser observado en todo momento. Lo llamó el panóptico. Se implementaron elementos de su diseño en prisiones reales con la esperanza de controlar y reformar mejor a los prisioneros.

Si Brin no se equivoca, ahora se encuentra en proceso de implementación a una escala algo mayor.

El caso de la videovigilancia en Gran Bretaña sugiere una razón: según los informes británicos, proporciona una forma efectiva y barata de combatir el crimen. En EE.UU., hace mucho que se han utilizado cámaras en los centros comerciales para disuadir de robar. Más recientemente han comenzado a usarse para atrapar a conductores que no paren en rojo. Si bien ha habido desafíos con respecto a la privacidad, parece probable que la práctica se extienda.

Evitar delitos no es el único beneficio de la vigilancia. Piensa en el problema de controlar las emisiones de los coches. Actualmente se impone un máximo fijado a todos los coches, exige que se inspeccione a todos, incluyendo los coches que casi seguro que aprobarán, y no proporciona un incentivo para evitar selectivamente las emisiones en sitios y momentos en que son particularmente dañinas.

Uno podría construir un sistema mucho mejor usando tecnología moderna. Coloca detectores no humanos que midan las emisiones haciendo brillar un rayo de luz a través de los escapes de un automóvil que pase; identifica el automóvil mediante una foto de la matrícula. Multa al dueño por la cantidad de emisiones y, en un sistema más sofisticado, por cuándo y dónde se emitió[20].

Otra aplicación de la vigilancia a larga escala con la que ya se está experimentando se aprovecha del hecho de que los móviles emiten continuamente señales de posición, irrastreables y producidas en el proceso de seguir el rastro de con qué torre deberían comunicarse. Observando las señales de los teléfonos de los conductores, es posible observar el tráfico. Es una información muy útil si quieres aconsejar a los conductores que bordeen un atasco, o para localizar un accidente por medio de los grupos de teléfonos resultantes. Actualmente es información anónima: se puede localizar un teléfono, pero no

[20] Para más detalles, véase Foldvary y Klein (2003).

identificar a su dueño. A medida que la tecnología evolucione, esto podría cambiar.

Ninguna de estas útiles aplicaciones de la tecnología presentan, a primera vista, una amenaza seria a la privacidad. Pocos considerarían objetable tener a un agente de policía por un parque o en una esquina de la calle, en busca de ladrones de bolsos y similares. Las videocámaras en postes son simplemente una forma más cómoda de hacer lo mismo. Las cámaras para los semáforos en rojo, o vigilancia fotométrica de los escapes de un coche son sustitutos más baratos y efectivos de los agentes de tráfico y las inspecciones de las emisiones. ¿Cuál es el problema?[21]

El problema viene cuando combinamos esta tecnología con otras. Un policía en la esquina podría verte, podría incluso recordarte, pero no tiene forma de combinar todo lo que ve con todo lo que ve otro policía y, así, reconstruir tu vida diaria. Una videocámara produce un registro permanente. Ahora es posible programar un ordenador para identificar a una persona a partir de una foto de su cara. Eso significa que las cintas producidas por las cámaras de vigilancia se podrán convertir en un registro de dónde se vio cuándo a gente en particular. Añade la capacidad del procesamiento de datos moderno para rastrear cantidades ingentes de información y tenemos la posibilidad de un mundo en que gran parte de lo que haces es un libro abierto para cualquiera con acceso a los registros apropiados. Suma a eso la capacidad de los ordenadores para identificar patrones sospechosos de comportamiento, algo con lo que ya se está experimentando en varios sitios, y los que controlan la tecnología pueden no solo mirar a todo, sino saber dónde mirar.

Hasta ahora hemos estado discutiendo el uso legal de la tecnología de vigilancia, en su mayoría por Gobiernos, algo que ya sucede en una escala sustancial y que es probable que aumente en un futuro cercano.

---

[21] La vigilancia del tráfico sugiere en el presente cómo podría ser la vigilancia de la gente en el futuro, ya que leer una matrícula, transpondedor o el sello electrónico de peaje es más sencillo que reconocer una cara.

Un asunto relacionado es el uso de la tecnología de vigilancia, legal o ilegalmente, en fiestas privadas. Mucha gente posee videocámaras y esas cámaras se están volviendo cada vez más pequeñas; incluso cada vez más gente posee móviles equipados con ellas. Uno puede imaginarse, dentro de una o dos décadas, una videocámara barata con el tamaño y las características aerodinámicas de un mosquito. El propietario de unas pocas docenas de ellas podría recopilar un montón de información sobre sus vecinos, o cualquier otra persona.

Por supuesto, es probable que el desarrollo tecnológico, en esta área como en otras, mejore la defensa tanto como el ataque. Las posibles defensas contra tal espionaje abarcan desde interferir en las transmisiones como libélulas autómatas programadas para cazar y destruir los videomosquitos. Esas tecnologías podrían posibilitar, incluso en un mundo en que todas las actividades públicas fueran fácilmente observables, el mantenimiento de una zona de privacidad en la casa de uno.

Pero podría ser que no. Ya hemos tenido casos en los tribunales sobre si es o no un registro deducir que hay marihuana creciendo en una casa usando un detector infrarrojo para medir su temperatura desde fuera. Ya tenemos tecnologías que posibilitan escuchar una conversación haciendo rebotar un rayo láser de una ventana y reconstruyendo a partir de las vibraciones medidas del cristal los sonidos que las causan. Incluso si no es posible espiar directamente en la vida privada, desarrollos ulteriores en esta línea podrían hacer posible lograr el mismo objetivo indirectamente.

Demos por hecho, por el momento, que el ataque vence a la defensa, que no se puede evitar que otra gente te espíe. ¿Qué opciones quedan?

Brin argumenta que la privacidad ya no será una de ellas. De forma más interesante, argumenta que podría ser bueno. Propone como alternativa a la privacidad la carencia universal de privacidad: la sociedad transparente. La policía puede vigilarte, pero alguien los está vigilando. Todo el sistema de videocámaras, incluidas las cámaras de

toda comisaría, es públicamente accesible. Haz click en la página web adecuada (leída, presumiblemente, desde un dispositivo inalámbrico). Los padres pueden tener vigilados a sus hijos, los hijos a sus padres, un esposo a otro, los empresarios a los empleados y viceversa, los periodistas a los policías y políticos.

El lado positivo de la transparencia

Muchos años atrás fui testigo de un tiroteo; un resultado fue la oportunidad de entablar cierta conversación espontánea con policías. Uno de ellos me aconsejó que, si se diera que alguna vez disparara a un ladrón, había dos cosas de las que debería asegurarme: que acabara muerto y que el cuerpo terminara dentro de mi casa.

El consejo tenía buena intención y quizás era sensato: bajo la ley estadounidense, un propietario se encuentra en una posición legal mucho más fuerte al matar a un intruso dentro de su casa que fuera, y un hombre muerto no puede dar su lado de la historia. Pero también era, al menos implícitamente, un consejo para cometer un crimen. Ese incidente, y uno menos amigable en otra jurisdicción donde estuve brevemente bajo arresto por perturbar la paz (mi infracción real fue ser cómplice de otro al pedir a un policía su número de placa), me convenció de que al menos algunos ejecutores de la ley, incluso aquellos que intentan sinceramente evitar delitos, tienen una visión elástica de la aplicación de la ley hacia ellos mismos y sus amigos. El problema es lo bastante viejo como para ser sujeto a una etiqueta latina: Qui custodes ipsos custodiet?, «¿Quién guardará a los guardianes?»

La sociedad transparente ofrece una posible solución. Piensa en el caso de Rodney King. Un grupo de policías capturó a un sospechoso y le pegó una paliza: una secuencia de hechos perfectamente ordinarios en muchas partes del mundo, incluidas algunas de los Estados Unidos. Desgraciadamente para la policía, un testigo grabó la paliza en video,

con el resultado de que varios de los agentes acabaron en prisión. Ha habido una serie de casos similares desde entonces. Los agentes ejecutores de la ley, decidiendo lo lejos que pueden ir más allá de lo que el público podría aprobar, tienen que tener en cuenta la posibilidad de que alguien podría tener una cámara de video apuntándoles. En el mundo de Brin, todo agente ejecutor de la ley sabe que se encuentra bajo cámara indiscreta todo el tiempo y se comporta en consecuencia.

Es una visión intrigante y podría pasar. Pero hay problemas.

Transparencia selectiva

El primero es llegar ahí. Si la transparencia llega, como está llegando en Inglaterra, en forma de cámaras en postes instaladas y operadas por el Gobierno, la versión de Brin no parece probable. Toda la información fluirá a través de maquinaria controlada por algún nivel del Gobierno. Quien quiera que esté al cargo puede argumentar plausiblemente que, aunque mucha de la información puede y debe hacerse accesible públicamente, debería haber límites. E incluso si no argumentan a favor de los límites, todavía pueden imponerlos. Si la policía monta cámaras en las comisarías, pueden preparar que unas pocas áreas se queden sin cubrir accidentalmente. Si el FBI está a cargo de una red nacional, y según se ha visto en el pasado lo estará, puede asegurarse de que parte de la información generada sea accesible solo a aquellos en quienes confían que no harán un mal uso de ella. La mayoría de los cuales trabajan para el FBI.

La situación se vuelve más interesante en un mundo en que el progreso tecnológico posibilita la vigilancia privada a escala global, de forma que toda localización donde podrían suceder cosas interesantes, incluida la comisaría, tiene moscas en la pared vigilando lo que sucede e informando a sus dueños. Es improbable que un individual privado, incluso una gran corporación, intente el tipo de vigilancia universal que Brin imagina para su sistema público, así que cada individuo recibirá

información solo sobre una pequeña parte del mundo. Pero si esa información es valiosa para los otros, puede compartirse. Los Gobiernos podrían intentar restringir este reparto. Pero en un mundo de privacidad férrea será difícil hacerlo, puesto que en tal mundo las transacciones de información serán invisibles para las partes de fuera. Combinando ideas de varios capítulos de esta sección, uno puede imaginar un futuro en que la sociedad transparente de Brin se produzca no por el Gobierno, sino por la vigilancia privada.

Es probable que una red de espías universal sea una proposición cara, especialmente si incluyes el coste del procesamiento de información: reconocimiento facial de cada imagen producida y análisis de los datos resultantes. Ni un solo individuo, probablemente ni una organización, encontrará de su interés asumir ese coste para producir información para su propio uso, aunque un Gobierno podría. La información se producirá privadamente solo si el productor puede usarla él mismo y vendérsela a otros. Así que una exigencia clave para una sociedad transparente generada de forma privada es un mercado de información bien organizado[22].

El lado negativo de la transparencia

Siguiendo a Brin, he presentado la sociedad transparente como un paso hacia el futuro, posibilitado por videocámaras y ordenadores. Uno podría, en cambio, verlo como un paso hacia el pasado. La privacidad que la mayoría de nosotros damos por hecho es, hasta un cierto grado, una novedad, un producto de las rentas en aumento de los últimos siglos. En un mundo en que mucha gente compartía una sola residencia, donde era probable que una cama en una posada fuera a ser compartida por dos o tres extraños, la transparencia no necesitaba videocámaras.

---

[22] De lo contrario, una sociedad transparente podría producirse por algo análogo a un proyecto gratuito para producir software. Cada participante contribuye con la información de sus cámaras y tiene acceso a la información de las cámaras de todos.

Para un ejemplo más extremo, piensa en una sociedad primitiva como Samoa. Múltiples familias comparten una sola casa. Sin paredes. Aunque no haya Internet para difundir la información, la comunidad es lo suficientemente pequeña para hacer del cotilleo un sustituto adecuado. Se entrena a los niños desde pequeños a no hacer ruido. Los adultos rara vez expresan hostilidad[23]. La mayor parte del tiempo, alguien puede estar observando, así que cambias el comportamiento en consecuencia. Si no quieres que tus vecinos sepan lo que estás pensando o sintiendo, evitas expresarlo claramente con palabras o con la expresión facial. Has adaptado tu vida a una sociedad transparente.

En última instancia, esto se reduce a dos estrategias que nos resultan familiares en otros contextos. Una es no hacer saber a nadie tus secretos: vivir como en una isla. La otra es comunicarlos en código, usar palabras o expresiones que tus íntimos interpreten correctamente y los otros no. Para una versión más moderada de la misma propuesta, piensa en los padres que hablan los unos a los otros en una lengua extranjera cuando no quieren que sus hijos comprendan lo que están diciendo, o una traducción del siglo XIX de una novela china con la que me encontré una vez, con los pasajes pornográficos traducidos al latín en vez de al inglés.

En la futura sociedad transparente de Brin, muchos de nosotros estaremos menos dispuestos a expresar nuestras opiniones a jefes, empleados, ex o actual marido en cualquier sitio público. La gente se volverá menos expresiva y más reservada, más sosa en la conversación o críptica. Si algunos espacios todavía son privados, más vida social pasará a hacerse en ellos. Si todo sitio es público, habremos vuelto atrás al menos varios siglos, posiblemente varios milenios.

[23] Freeman, 1983.

¿QUÉ ES LA PRIVACIDAD Y POR QUÉ LA QUEREMOS?

Piensa en «privacidad» como taquigrafía para una capacidad individual para controlar que otras personas accedan a su información. Si tengo un derecho legal para que no me pinches el teléfono, pero no puedo ejecutarlo (la situación actual para los que usan teléfonos inalámbricos sin encriptación), entonces tengo poca privacidad en mis llamadas. Tengo una privacidad casi completa respecto a mis propios pensamiento, incluso si es perfectamente legal que otra gente use las tecnologías disponibles (escuchar mi voz y observar mis expresiones faciales) para intentar sacar lo que estoy pensando. La privacidad en este sentido depende de una variedad de cosas, incluyendo la ley y la tecnología. Si alguien inventara una forma sencilla y precisa de leer las mentes, la privacidad se reduciría radicalmente, incluso si no hubiera cambio en mis derechos legales[24].

Una razón para definir así la privacidad es que estoy interesado en sus consecuencias, en las maneras en que mi capacidad de controlar información sobre mí reporta beneficios o daños hacia mí y los otros, sea cual sea la fuente de esa capacidad. Otra es que estoy interesado en las formas en que es probable que la tecnología cambie la capacidad de un individuo para controlar dicha información. Por tanto, en cambios en la privacidad debidos a fuentes distintas de los cambios en mis derechos legales.

---

[24] Este podría no ser un ejemplo completamente hipotético. Ahora hay algunas pruebas de que las exploraciones cerebrales se pueden usar para indicar si alguien está mintiendo: http://www.futurepundit.com/archives/003548.html. A medida que comprendamos mejor el cerebro, podría ser posible decir más sobre lo que la gente está pensando observando lo que está pasando en sus cerebros. También hay alguna prueba de que podría volverse posible usar exploraciones cerebrales para identificar a los psicópatas, lo que plantea cuestiones adicionales: http://www.futurepundit.com/archives/004209.html.

Contra la privacidad[25]

Mucha gente se toma molestias para reducir lo que otros pueden descubrir sobre ellos. Mucha gente, a veces la misma, hace un esfuerzo para obtener información sobre otra gente. Ello plantea una pregunta interesante: En la red, ¿es bueno o malo un incremento de la privacidad? ¿Gano más con que seas incapaz de descubrir cosas sobre mí que lo que pierdo con ser incapaz de descubrir cosas sobre ti?

La mayor parte de la gente parece pensar que la respuesta es afirmativa. Es común ver alguna tecnología, norma legal o producto nuevo atacado por reducir la privacidad, es raro ver atacado algo por incrementar la privacidad. ¿Por qué?

La razón por la que valoro mi privacidad es directa: la información sobre mí en las manos de otra gente les permite a veces ganar a mi costa. Podrían hacerlo robándome mi propiedad (si, por ejemplo, saben que no estoy en casa). Podrían hacerlo obteniendo términos más favorables en una transacción voluntaria (si, por ejemplo, saben justo cuánto estoy dispuesto a pagar por la casa que venden). Podrían hacerlo evitando que robe su propiedad (por ejemplo, no contratándome como tesorero de una compañía tras descubrir que soy un desfalcador que fue condenado).

La información sobre mí en las manos de otra gente también podría beneficiarme (por ejemplo, la información de que soy honesto y competente). Pero la privacidad no evita que esa información les esté disponible. Si tengo control sobre la información acerca de mí mismo, puedo difundirla cuando, y solo cuando, hacerlo sea de mi interés[26].

---

[25] Para una discusión más extensa de los asuntos de este capítulo, véase Friedman, 2000, en el que empleo el término «derechos de privacidad» para lo que aquí llamo privacidad. Para una discusión más general de los derechos desde una perspectiva relacionada, véase Friedman, 1994. Mi privacidad mental no es del todo completa, pero la única excepción importante es mi mujer.

[26] Una posible excepción es el caso en que la información relevante es negativa (digamos, el hecho de que no me he declarado en bancarrota) y las terceras partes no tienen forma de saber si he actuado para suprimirla. Si los individuos tienen control sobre información de esta

Mis ejemplos han incluido uno (en el que mi privacidad me protege del robo) en que la privacidad producía un beneficio neto, ya que la ganancia de un ladrón es normalmente menor que la pérdida de la víctima. Incluían una (donde mi privacidad me permitía robar a otros) en que la privacidad producía una pérdida neta. E incluían un caso (negocio) en que el efecto neto parecía un empate, ya que lo que perdí lo ganó otro[27].

Si miramos más cuidadosamente, ese tercer caso es probablemente una ganancia neta. Uno de los riesgos de negociar es la ruptura del negocio cuando un vendedor sobreestima el precio que un vendedor está dispuesto a pagar o un comprador realiza el error correspondiente y el acuerdo fracasa, con lo que ambas partes están peor que si cada uno hubiera leído mejor al otro. La privacidad hace más difícil saber cosas sobre los otros (los compradores y vendedores están, después de todo, representando mal de forma deliberada lo que están dispuestos a ofrecer o aceptar con la esperanza de alcanzar un acuerdo mejor), haciendo la ruptura del negocio más probable. Parece como si la privacidad produjera, de media, una pérdida neta en las situaciones en que las partes estén buscando información sobre la otra para mejorar los términos de una transacción voluntaria, ya que aumenta el riesgo de romper el negocio[28]. En las situaciones que involucran transacciones

---

índole, entonces la ausencia de pruebas de que me he declarado en bancarrota no proporciona pruebas de que no lo haya hecho, de forma que los prestatarios que no se han declarado en quiebra en el pasado estarán mejor en un mundo en que los derechos de privacidad con respecto a información así son débiles. El problema desaparece si puedo llevar a cabo una acción observable (como firmar una dispensa de los derechos de privacidad legal relevantes que se pueda ejecutar legalmente) que demuestre que la información no se está suprimiendo.

[27] Muchos de los argumentos que se han hecho en esta parte del capítulo se pueden encontrar, de alguna forma distinta, en Posner, 1978, «The Right of Privacy», y Posner, 1978, «An Economic Theory of Privacy», quien encuentra débil la defensa de la conveniencia general de la privacidad.

[28] Este podría no ser el caso si nos encontramos a menudo enfrentados con situaciones donde mis ganancias de la ganga me proporcionen el incentivo para generar información que también sea de valor para otros. Tiene poco sentido gastar tiempo y dinero prediciendo un aumento en los precios del trigo si todo cuanto descubres se revela a vendedores potenciales antes de que tengas una oportunidad de comprarles. Es, de alguna forma, un caso extraño, porque, mientras que la especulación exitosa es socialmente útil y rentable, no hay una conexión particular entre los dos factores, como está señalado en Hirschleifer, 1971. De ahí la oportunidad para que la ganancia especulativa produzca o demasiado o demasiado poco

involuntarias, la privacidad produce una ganancia neta si se está usando para proteger otros derechos (dando por hecho que esos derechos se han definido de una forma que haga deseable su protección) y una pérdida neta si se está usando para violar otros derechos (dando por hecho lo mismo). No hay una razón obvia por la que la primera situación deba ser más común que la última. Así que, mientras que está claro que estoy a favor de tener privacidad, no está claro por qué debería esperar que mis ganancias de tener privacidad sean mayores que las pérdidas de que tengas privacidad, por qué la gente debería considerar la privacidad, generalmente, como algo bueno.

Privacidad y Gobierno

Habría sido imposible medir con una exactitud tolerable el impuesto sobre una tienda en función del comercio que se realiza en ella, sin una inquisición tal que habría sido totalmente inaguantable en un país libre.

Explicación de Adam Smith sobre por qué es inviable un impuesto sobre las ventas

(Riqueza de las naciones, libro V, capítulo II, punto 2, artículo II)

El estado de la fortuna de un hombre varía de un día a otro, y sin una inquisición más intolerable que cualquier impuesto, y renovada al menos una vez cada año, solo puede suponerse.

---

incentivo para obtener la información necesaria. Una segunda cualificación es que podría no ser el caso si hubiera alguna forma completamente verificable de desprenderme de mi privacidad, de hacerte saber el precio más alto que estaba dispuesto a pagar a cambio de que me hagas saber el precio más bajo que ibas a aceptar. Esto nos lleva de vuelta a un argumento realizado en una nota anterior: la dificultad de transmitir información creíble en un contexto en que tenga el poder de seleccionar qué información se transmite.

Explicación de Smith de por qué es inviable un impuesto sobre la renta

(Riqueza de las naciones, libro V, capítulo II, punto 2, artículo IV)

Aunque las partes privadas se meten de vez en cuando en transacciones involuntarias como el robo, la mayoría de nuestras interacciones con los otros son voluntarias. Los Gobiernos se embarcan en transacciones involuntarias en una escala enormemente mayor. Y los Gobiernos casi siempre tienen una superioridad apabullante de fuerza física sobre el ciudadano individual. Mientras que puedo protegerme de mis compañeros ciudadanos con cerraduras y alarmas antirrobo, puedo protegerme de los actores del Gobierno solo manteniendo la información sobre mí fuera de sus manos[29].

Las implicaciones dependen de la visión del Gobierno de uno. Si el Gobierno es el equivalente moderno del rey-filósofo de Platón, la privacidad individual simplemente hace más difícil que el Gobierno haga buenas obras. Si, por otra parte, un Gobierno es simplemente una banda criminar particularmente grande y bien organizada que roba tanto como puede de nosotros, la privacidad individual contra el Gobierno es buena, sin ambigüedad. La mayoría de los estadounidenses parecen, a juzgar por las concepciones expresadas sobre la privacidad, estar lo bastante cercanos a la privacidad para considerar la privacidad contra el Gobierno algo completamente deseable, con una excepción para casos en que creen que la privacidad podría usarse para ocultar delitos sustancialmente más serios que la evasión de impuestos.

Desde esta perspectiva, un problema con la sociedad transparente de Brin es el enorme riesgo de los inconvenientes. Usada con supuestos menos optimistas que los suyos, la tecnología podría posibilitar una

---

[29] Una propuesta alternativa podría ser la actividad política: presionar al Congreso o hacer contribuciones al fondo de caridad de la policía o participar en una revolución. Para la mayor parte de los individuos en una sociedad grandes, incluido yo, estas tácticas rara vez merecen su coste.

tiranía que Hitler o Stalin envidiarían. Incluso si aceptamos el supuesto optimista de Brin de que los ciudadanos están tan bien informados sobre la policía como la policía sobre los ciudadanos, es la policía la que tiene las pistolas. Saben si estamos haciendo o diciendo algo que desaprueben y responden en consecuencia, arrestando, metiendo en la cárcel, quizás torturando o ejecutando a sus oponentes. Tenemos el privilegio de vigilar. ¿Por qué deberían objetar? Las ejecuciones públicas son una vieja tradición, diseñada en parte para disuadir a otra gente de hacer lo que podría ejecutarles.

No se sigue que la prescripción de Brin esté equivocada. Su argumento, después de todo, es que la privacidad no debería ser simplemente una opción, o porque los beneficios visibles de la vigilancia son muy grandes o porque la tecnología hará imposible evitarla. Si tiene razón, su sociedad transparente podría al menos ser mejor que la alternativa: la vigilancia a la que solo tengan acceso los que están en el poder, un panóptico universal con el Gobierno como guardián de la prisión.

DI QUE NO ES ASÍ

Hasta ahora he ignorado un problema interesante con el mundo de Brin: la verificación. Piensa en el siguiente drama en los tribunales:

Mi mujer me ha lanzado una demanda de divorcio por adulterio. En apoyo de su afirmación, presenta cintas de video grabadas por cámaras ocultas, que me muestran haciendo el amor a tres mujeres distintas. Ninguna de ellas era ella.

Mi abogado pide posponerlo para investigar las nuevas pruebas. Cuando el tribunal vuelve a reunirse, envía su propia cinta. El jurado observa a mi mujer haciendo el amor, consecutivamente, con Humphrey Bogart, Napoleón, su abogado y el juez. Cuando se recupera el orden en el tribunal, mi abogado presenta al juez la dirección de la empresa de efectos de video que produjo la cinta.

Con la tecnología moderna no necesito, o al menos pronto no necesitaré, tu cooperación para hacer una película sobre ti haciendo cosas; una selección razonable de fotografías valdrá. Como Hollywood demostró con Roger Rabbit, es posible combinar personajes reales y de dibujos animados en lo que parece una sola cinta. En el futuro próximo el equivalente, usar animaciones convincentes de gente real, será algo que un aficionado competente podrá producir en su escritorio. Podríamos ver por fin a John F. Kennedy haciendo el amor a Marilyn Monroe, sucediera o no.

En ese mundo, la distinción entre lo que sé y lo que puedo probar se vuelve crítica. Nuestro mundo podría estar lleno de videomosquitos, cada uno informando a su dueño y cada dueño echando la información a una reserva común, pero algunos podrían estar mintiendo. Cuando saco información de la reserva, no tengo forma de saber si creerla.

Hay posibles arreglos tecnológicos, maneras de usar la tecnología de la encriptación para construir una cámara que señalice su salida digitalmente, demostrando que la secuencia se tomó con esa cámara en un momento particular. Pero es difícil diseñar un sistema que no pueda resultar debilitado por el propietario de la cámara. Incluso si podemos probar que una cámara particular grabó una cinta de mí haciendo el amor a seis mujeres, ¿cómo sabemos si lo hizo mientras me apuntaba a mí o a una pantalla de video que mostraba el trabajo de un estudio de animación? El potencial para la falsificación debilita significativamente la capacidad de la tecnología de vigilancia para producir información verificable.

Para muchos fines, la información inverificable bastará: si mi esposa quiere saber de mi infidelidad, pero no necesita probarla. Siempre que el Gobierno que dirija un sistema de vigilancia pueda confiar en su propia gente, puede usar ese sistema para detectar delitos o expresiones de opinión políticamente no populares. Y la prueba en video todavía se podrá usar en juicios, siempre que se acompañe de las pruebas suficientes para demostrar dónde y cuándo se tomó y que no se ha mejorado desde entonces. Se vuelve más creíble con la redundancia:

cinco videomosquitos, pertenecientes a distintos dueños, mostrando los mismos sucesos.

¿DEBERÍAMOS ABOLIAR EL DERECHO PENAL?

Las sociedades modernas tienen dos tipos diferentes de normas legales: el derecho penal y el derecho de la responsabilidad civil, que hacen esencialmente la misma cosa. Alguien hace algo que daña a otros. Se le acusa, juzga y condena, y como resultado le pasa algo malo, lo que proporciona el incentivo de no hacer cosas así a otra gente. En el sistema penal, el procesamiento judicial está controlado y fundado por el Estado, en el sistema de responsabilidad civil, por la víctima. En el sistema penal, un acuerdo se llama plea bargain [acuerdo táctico entre fiscal y defensa para agilizar los trámites judiciales, en el derecho de la Common Law]; en el sistema de responsabilidad civil, arreglo extrajudicial. El derecho penal proporciona una gama de castigos algo diferentes (no es posible ejecutar a alguien por responsabilidad civil, por ejemplo, aunque era posible que algo muy parecido a un procesamiento judicial por responsabilidad civil llevara a la ejecución según la ley inglesa hace unos pocos siglos) y opera según normas legales algo diferentes[30]. Pero en líneas generales, los dos sistemas no son más que dos maneras ligeramente distintas de hacer lo mismo.

Esto plantea una pregunta obvia: ¿hay alguna buena razón para tener ambas? ¿Podríamos, por ejemplo, estar mejor aboliendo el derecho civil al completo y, en lugar de él, hacer que las víctimas de los delitos demanden a los delincuentes?

---

[30] En el siglo XVIII, Blackston describió la apelación del delito, una acción privada para la pena criminal (por supuesto, capital), como algo que todavía estaba en los libros, pero que empezaba a caer en desuso. Como lo describió, «en una acusación, que se realiza a demanda del rey, el rey puede perdonar y anular la ejecución; en una apelación, que se realiza a demanda de un sujeto privado... el rey ya no puede perdonarlo más de lo que puede anular los daños recuperados en una agresión.» (Blackstone, 1979, V4, ch. 23, p. 311.) Véase Friedman, 2001, cap. 14, 15, 18, en http://www.daviddfriedman.com/laws order/index.shtml.

Un argumento contra un sistema de pura responsabilidad civil es que algunos delitos son difíciles de detectar. Una víctima podría llegar a la conclusión de que atrapar y procesar judicialmente al infractor cuesta más de lo que vale, especialmente si resulta que el infractor no tiene suficientes activos como para pagar daños sustanciales. De ahí que algunas categorías de delito pudieran quedar sin castigo por rutina.

En el mundo de Brin ese problema desaparece. Todo robo con violencia está grabado. Si el ladrón decide llevar una máscara mientras cometa el delito, podemos seguirle el rastro por la grabación antes o después hasta que se la quite. Mientras que un delincuente lo suficientemente ingenioso podría encontrar una forma de eludir este problema, la mayor parte de los delitos con los que ahora se las ve el derecho penal serían casos en que la mayoría de los hechos se conocen y solo quedan por determinar las implicaciones legales. El delito normal se vuelve muy parecido a la responsabilidad civil normal: digamos, un accidente de coche, donde, excepto en el caso de darse a la fuga, que es un crimen, la identidad de la parte y muchos de los hechos relevantes son información pública. En ese mundo, podría tener sentido abolir el derecho penal y cambiar todo a la alternativa descentralizada, controlada de forma privada. Si alguien te roba el coche, compruebas la grabación para identificar al ladrón, entonces lo denuncias por el coche más un pago razonable por el tiempo y molestias en recuperarlo.

Como muchas ideas radicales, esta parece mucho menos radical si uno está familiarizado con la historia relevante. Los sistemas legales en que algo similar al derecho de responsabilidad civil se enfrentaba con lo que consideramos delitos (en los que, si matabas a alguien, su pariente te demandaba) son comunes en los registros históricos[31]. Incluso tan tarde como en el siglo XVIII, mientras que el sistema legal inglés distinguía entre las responsabilidades civiles y penales, ambas se perseguían judicialmente de forma privada, normalmente por la víctima[32]. Una

[31] Friedman, 1979, en http://www.daviddfriedman.com/Academic/Iceland/Iceland.html. Un asesino podía ser demandado por los familiares de su víctima y, si perdiera el caso y se negara a pagar los daños, se arriesgaba a que se le diera caza y lo mataran.

[32] Friedman, 1995, en http://www.daviddfriedman.com/Academic/England

posible explicación para el cambio a un sistema de procesamiento judicial moderno y público del derecho penal es que era una respuesta al anonimato en aumento que acompañaba al cambio de una sociedad urbana más urbana a finales del siglo XVIII y principios del XIX[33]. Las tecnologías que invierten ese cambio podrían justificar una inversión de los cambios legales ligados a él.

DONDE CHOCAN LOS MUNDOS

En el capítulo 4 he descrito un ciberespacio con más privacidad que la que hoy tenemos. En este capítulo he descrito un espacio real con menos. ¿Qué sucede si tenemos ambas opciones?

No sirve de nada usar una fuerte encriptación para mi correo electrónico si un videomosquito está sentado en la pared viéndome escribir. Así que la privacidad férrea en una sociedad transparente necesita alguna manera de guardar la interfaz entre mi cuerpo en el espacio real y el ciberespacio. No es un gran problema en la versión en que las paredes de mi casa son todavía opacas[34]. Es un problema serio en la versión en que todos los sitios son, de hecho si no de derecho, públicos. Una solución de baja tecnología es escribir bajo una capucha. Una solución de alta tecnología es algún vínculo entre mente y

---

18thc./England 18thc.html. Alguna ejecución legal se realizaba mediante asociaciones de acusación, organizaciones privadas para procesar los delitos cometidos contra sus miembros (los que pagan las cuotas). Uniéndose a una asociación de esta naturaleza (ser miembro era una información pública), un individuo se comprometía previamente al procesamiento de delitos cometidos contra él, lo que hacía de la disuasión un bien privado.

[33] Davies, 2002, defiende que el sistema de procesamiento privado lidiaba exitosamente con los problemas de la urbanización y se reemplazó por la política pública por otras razones, relacionadas con evitar la insurrección y con eliminar las causas del delito reformando a los pobres.

[34] Todavía tengo que preocuparme por las tecnologías para escuchar el sonido del teclado y deducir de ahí lo que estoy escribiendo, u observando señales electromagnéticas desde mi pantalla de ordenador a una distancia.

máquina que no vaya a través de los dedos o de cualquier otra cosa visible para un observador externo[35].

El conflicto entre la transparencia en el espacio real y la privacidad en el ciberespacio va también en la otra dirección. Si estamos lo bastante preocupados por que otra gente escuche lo que decimos, una solución es encriptar la conversación cara a cara. Con los dispositivos inalámbricos apropiados, hablo en un micrófono de garganta o escribo en un teclado virtual (manteniendo las manos en los bolsillos). Mi ordenador de bolsillo encripta el mensaje con tu clave pública y lo transmite a tu ordenador de bolsillo, que desencripta el mensaje y lo muestra en tus gafas de realidad virtual. Para asegurarte de que nadie está leyendo las gafas por encima de tu hombro, te proporcionan la imagen no mostrándola en una pantalla, sino usando un láser diminuto para escribir en tu retina. Con suerte, el interior de tu ojo es todavía un espacio privado.

Podríamos acabar en un mundo en que las acciones físicas sean completamente públicas; las transacciones de información, completamente privadas. Tiene algunas características atractivas. Los ciudadanos privados todavía serán capaces de aprovecharse de la privacidad férrea para localizar a un asesino a sueldo, pero contratar uno podría costar más de lo que estén dispuestos a pagar, ya que en un mundo lo bastante transparente se detectan todos los delitos. Todo asesino a sueldo ejecuta un encargo y luego va directo a la cárcel.

¿Y la interacción entre estas tecnologías y el procesamiento de datos? Por una parte, es el proceso de datos moderno lo que hace de la sociedad transparente una amenaza de gran calibre. Sin él, no importaría mucho si grabaras en video todo lo que sucediera en el

---

[35] http://www.cnn.com/2004/TECH/12/07/computer.thought.reut/index.html describe un experimento en el que los individuos controlaban un ratón pensando. Llevaban un gorro con sesenta y cuatro electrodos para detectar la actividad cerebral. En el otro extremo, los *keyloggers* son una manera de acabar con la privacidad informática que ya está en uso (es un *software* que registra las teclas que pulsas cuando utilizas el ordenador, las graba en un archivo que luego se puede usar para reconstruir lo que hacías; piensa en ello como un mosquito virtual con video que te observa mientras escribes). Para el primer caso judicial relacionado con los *keyloggers*, véase http://news.com.com/2100–1023-983717.html.

mundo, ya que nadie podría encontrar jamás las seis pulgadas particulares de la grabación que deseara en los millones de millas que se producirían cada día. Por otra parte, las tecnologías que apoyan la privacidad férrea proporcionan la posibilidad de restablecer la privacidad, incluso en un mundo con proceso de datos moderno, evitando que la información sobre tus transacciones llegue a otro salvo a ti. Este es un tema al que volveremos en un capítulo posterior, cuando discutamos el dinero electrónico, una idea soñada en parte como manera de restaurar la privacidad transaccional.

PARTE TRES

HACER NEGOCIOS EN LÍNEA

SEIS

DINERO ELECTRÓNICO

Pago por cosas de una de las tres maneras distintas que hay: tarjeta de crédito, cheque o efectivo. Las primeras dos me permiten realizar pagos elevados sin tener que llevar grandes cantidades de dinero. ¿Cuáles son las ventajas de la tercera?

Una es que un vendedor no tiene que saber nada de mí para aceptar efectivo. Esto hace del dinero un medio mejor para las transacciones con extraños, especialmente extraños que se encuentran lejos. También lo convierte en un medio mejor para transacciones pequeñas, ya que usar efectivo evita los costes fijos de controlar a alguien para asegurarse de que realmente hay dinero en su cuenta corriente o que su crédito es bueno. También significa que el dinero no deja rastro en papel, lo que es útil no solo para los delincuentes, sino para cualquiera que quiera proteger su privacidad, un asunto cada vez más importante en un mundo en que el procesamiento de datos amenaza con hacer público cada detalle de nuestras vidas.

La ventaja del dinero es mayor en el ciberespacio, ya que es más probable que las transacciones con extraños, incluidos los extraños que estén lejos, tengan lugar en Internet que en mi barrio del espacio real. La desventaja es menor, ya que mi dinero electrónico se almacenaría en mi ordenador, que normalmente está en mi casa, y, por tanto, es menos vulnerable al robo que mi cartera.

A pesar de su utilidad potencial, aún no hay un equivalente al efectivo disponible en línea, aunque ha habido intentos fallidos de crearlo e intentos exitosos de crear algo cercano. La razón no es tecnológica: esos problemas se han solucionado. El motivo es, en parte, la hostilidad de los Gobiernos a la competición en el negocio monetario, y en parte la dificultad de establecer estándares, en este caso estándares monetarios privados. Espero que ambos problemas se resuelvan en algún momento de la próxima década o la siguiente.

Antes de discutir cómo podría funcionar un sistema de moneda electrónica, privada o gubernamental, merece la pena dar primero

como mínimo un ejemplo de por qué sería útil (para algo más importante que permitir que los hombres vean pornografía en línea sin que sus mujeres o jefes se enteres).

TROCEANDO EL SPAM

Mi correo electrónico contiene mucha información de interés. También contiene ¿PREPARADO PARA UNA CÓMODA MANERA DE SALIR DE LAS DEUDAS? Una Invitación Personal de obtén_dinero_real@BIGFOOT.COM, Has Sido Seleccionado... de friend@localhost.net, y una variedad de mensajes similares, de los que mi favorito ofrece «la respuesta a todas tus preguntas». Internet ha traído muchas cosas de valor, pero para la mayoría de nosotros el correo electrónico comercial no solicitado, más conocido como *spam,* no es una de ellas.

Hay una solución simple para este problema, tan simple que estoy sorprendido de que todavía no sea de uso común. La solución es poner un precio a tu buzón de correo electrónico. Dale a tu programa de correo una lista de la gente de la que desees recibir mensajes. Los mensajes de cualquiera que no esté en la lista se devolverán con una nota explicando que cobras cinco céntimos por leer correo de desconocidos, y la URL de la máquina de correo. Cinco céntimos es un coste trivial para cualquiera con algo que decir que es probable que quieras leer, pero cinco céntimos por diez millones de receptores es un coste bastante sustancial para alguien que manda correos a granel por la posibilidad de que un destinatario de diez mil pueda responder.

La máquina de sellos se encuentra localizada en una página web. Los sellos son dinero digital. Paga diez dólares de tu tarjeta de crédito y, a cambio, recibes doscientos sellos de cinco céntimos, cada uno información encriptada que puedes transferir a otro que pueda transferirla como respuesta.

Un sello virtual, a diferencia de un sello real, puede reutilizarse; se paga no por el coste de transmitir el correo, sino por el tiempo y molestias de leerlo, así que el pago va a mí, no a la oficina de correos. Puedo usarlo la próxima vez que quiera mandar un mensaje a un

extraño. Si un montón de extraños eligen mandarme mensajes, puedo acumular un excedente de sellos que al final se volverán a canjear por dinero.

Cuánto cobre depende de mí. Si odio leer mensajes de desconocidos, puedo fijar el precio en un dólar, o diez, o cien y recibir muy pocos. Si disfruto los correos basura, puedo fijar un precio bajo. Una vez se establezca dicho sistema, la misma gente que actualmente crea y alquila las listas de correo usadas para mandar *spam* añadirá otro servicio: una base de datos que siga el rastro de cuándo cobra cada objetivo potencial por recibirlo.

¿Qué gana la máquina de sellos? ¿Por qué querría alguien mantener un sistema así? Parte de la respuesta es señorazgo: el beneficio de acuñar dinero. Tras vender cien millones de sellos de cinco céntimos, tienes cinco millones de dólares de dinero. Si tus sellos son populares, muchos de ellos pueden estar en circulación mucho tiempo, con lo que dejan el dinero que las compró en tu cuenta bancaria acumulando intereses.

Además del uso libre del dinero de otra gente, hay una segunda ventaja. Si posees la máquina de sellos, también posees el muro detrás de ella: la página web que la gente visita para comprar sellos. Los anuncios de ese muro los verá mucha gente.

Una razón por la que esta solución al *spam* requiere dinero electrónico es que involucra un gran número de pagos muy pequeños. Sería muy patoso usar tarjetas de créditos: cada vez que recibiéramos un mensaje con un sello de cinco céntimos, tendrías que comprobar con el banco del emisor antes de leerlo que el pago fue correcto. Una segunda razón es la privacidad. Muchos de nosotros preferiríamos no dejar un registro completo de nuestra correspondencia con una tercera parte, algo que haríamos si usáramos tarjetas de crédito o algo similar. Lo que queremos no es simplemente dinero electrónico, sino dinero electrónico anónimo, alguna manera de realizar pagos que no proporcione información a terceras partes sobre quién ha pagado qué a quién.

CONSTRUIR DINERO ELECTRÓNICO

Supón que un banco quiere crear un sistema de dinero electrónico. El primer problema, y el más sencillo, es cómo proporcionar a la gente billetes virtuales que no puedan falsificarse.

La solución es una firma digital. El banco crea un billete que dice «Primer Banco del Ciberespacio: Páguese al portador un dólar en moneda estadounidense». Firma digitalmente el billete, usando su clave privada. Hace que la clave pública concordante esté globalmente disponible. Cuando vienes al banco con un dólar, te da un billete en forma de un archivo en un pincho. Transfieres el archivo al disco duro, que ahora tiene un billete de un dólar con el que comprar algo de otra persona en línea. Cuando recibe el archivo, comprueba la firma digital con la clave pública del banco.

El problema de gastar el doble

Hay un problema. Un gran problema. Lo que has obtenido con tu dólar no es un solo billete de dólar, sino un número ilimitado de ellos. Mandar una copia del archivo en pago a una transacción no lo elimina del ordenador, así que puedes mandarlo de nuevo a otro para comprar otra cosa. Y otra vez. Va a ser un problema para el banco cuando veinte personas entren a reclamar tu billete de dólar original.

Una solución es que el banco asigne a cada dólar su propio número de identificación y siga el rastro de cuáles ha gastado. Cuando un comerciante recibe tu archivo, lo manda al banco, que deposita el dólar correspondiente en su cuenta y añade su número a una lista de billetes que ya no son válidos. Cuando tratas de gastar una segunda copia del billete, el comerciante que lo recibe trata de cobrarlo, se le informa de que ya no es válido y no te manda sus bienes.

Esto soluciona el problema de gastar dos veces, pero también elimina la mayoría de las ventajas del dinero electrónico sobre las tarjetas de crédito. El banco sabe que ha emitido el billete 94602… a Alice, y sabe que vino de Bill, así que sabe que Alice compró algo de Bill, como lo habría sabido si hubiera usado una tarjeta de crédito.

La solución a este problema emplea lo que David Chaum, el criptógrafo holandés responsable de muchas de las ideas que subyacen en el dinero electrónico, llama *firmas ciegas*. Es una manera de que Alice, habiendo cogido un número de identificación aleatorio para un billete de un dólar, pueda ir al banco a firmar ese número (a cambio de pagar al banco un dólar) sin tener que decirle al banco cuál es el número que está firmando. Incluso si el banco no sabe el número de serie que firmó, tanto él como el comerciante que recibe el billete puede comprobar que la firma sea válida. Una vez se gasta el billete de un dólar, el comerciante tiene el número de serie, del que informa al banco, que puede añadirlo a la lista de números de serie que ahora son inválidos. El banco sabe que dio un dólar a Alice y que recibió un dólar de Bill, pero no sabe que son el mismo dólar. Así que no sabe que Alice compró algo a Bill. El vendedor tiene que comprobarlo con el banco y saber que el banco es digno de confianza, pero no tiene que saber nada del comprador.

Los lectores curiosos querrán saber cómo es posible que un banco firme un número de serie sin saber qué es. No puedo decírselo sin explicar primero las matemáticas de la encriptación en clave pública, lo que requiere más matemática de la que estoy dispuesto a asumir que tiene mi lector medio. Los que tengan curiosidad pueden encontrar las respuestas en las notas virtuales (www.daviddfriedman.com/Future_Imperfect.html), que contienen las explicaciones de tanto la encriptación en clave pública como las firmas ciegas.

Hasta ahora he estado dando por hecho que la gente que recibe dinero digital puede comunicarse con el banco que lo emite mientras tiene lugar la transacción, que ellos y el banco están conectados a Internet o algo similar. Esto no es una constricción seria si la transacción está teniendo lugar en línea. Pero el dinero digital podría ser útil para las transacciones en el espacio real, y el taxista o vendedor de perritos calientes podrían no tener aún una conexión de Internet.

La solución es otro truco astuto (Chaum se especializa en trucos astutos). Es una forma de dinero que contiene información sobre la persona a la que se emitió, pero solo revela la información si el mismo

billete de dólar se gasta dos veces. Para una explicación de cómo funciona esto, de nuevo tienes que ir a las notas virtuales.

Los lectores escépticos deberían estar más y más descontentos en este punto al decírseles que todo lo del dinero electrónico se hace por medio de matemáticas que no estoy dispuesto a explicar, algo que podrían traducir razonablemente como «cortina de humo». Para su beneficio, he inventado mi propia forma de dinero electrónico, una que tiene todas las características del real y que puede entenderse sin matemáticas más allá de la capacidad de reconocer los números. Es mucho menos cómodo que la versión de Chaum, pero mucho más fácil de explicar, y así proporciona al menos una prueba de la posibilidad del dinero electrónico real.

Dinero electrónico de baja tecnología

Creo aleatoriamente un número muy largo. Pongo el número y un billete de un dólar en un sobre y lo mando al Primer Banco de Ciberdinero. El PBC acuerda, en un comunicado público, hacer dos cosas con el dinero que recibe de esta manera:

1. Si alguien entra en el PBC y presenta el número, obtiene el billete asociado a ese número.

2. Si el PBC recibe un mensaje que incluye el número asociado con un billete de dólar que tiene en depósito, ordenando al PBC que lo cambie a un nuevo número, hará el cambio y publicará el hecho de la transacción en un tablón visible públicamente. El billete de dólar ahora se asociará al nuevo número.

Veamos cómo funciona:

Alice ha mandado un dólar al PBC, acompañado del número 59372. Ahora quiere comprar a Bill imágenes digitales por valor de un dólar, así que le manda el número por correo electrónico como pago. Bill escribe al PBC, mandándoles tres números: 59372, 21754 y 46629.

El PBC comprueba si hay un dólar en el depósito con número 59372: lo hay. Cambia el número asociado a ese billete por 21754, el segundo número de Bill. A la vez, publica en un tablón visible públicamente la declaración «Se ha aprobado la transacción identificada por 466629».

Bill lee ese mensaje, lo que le dice que Alice tenía de verdad un dólar en el depósito y ahora es suyo, así que le manda a ella imágenes digitales por valor de un dólar.

Alice ya no tiene un dólar, ya que, si trata de gastarlo de nuevo, el banco informará de que no está ahí: el PBC ya no tiene un dólar asociado con el número que ella conoce. Bill ahora tiene un dólar, ya que el dólar que Alice mandó originariamente se encuentra ahora asociado a un nuevo número y solo él y el banco saben cuál es. Está precisamente en la misma situación en la que Alice estaba antes de la transacción, así que ahora puede gastar el dólar en comprar algo de otra persona. Como un dólar en papel ordinario, el dólar del dinero electrónico de mi sistema pasa de mano a mano. Al final alguien que lo tiene decide si, en lugar de él, prefiere un dólar de dinero normal; lleva su número, el número al que el dólar original de Alice se encuentra ahora asociado, al PBC y lo cambia por un billete de dólar.

Mi dinero electrónico puede ser de baja tecnología, pero cumple todas las exigencias. El pago se realiza mandando un mensaje. El pagador y el beneficiario no necesitan saber nada sobre la identidad del otro más allá de la dirección a la que mandar el mensaje. El banco no necesita saber nada de ninguna de las partes. Cuando el billete entró originariamente, la carta no tenía nombre, solo un número identificativo. Cada vez que cambiaba de manos, el banco recibía un correo, pero no tenía información sobre quién lo mandaba. Cuando acaba la cadena de transacciones y alguien viene al banco para recoger el billete, no necesita identificarse; incluso si el banco puede identificarle de alguna forma, no tiene forma de identificar a otros miembros de la cadena. El dólar virtual de mi sistema es tan anónimo como los dólares en papel de mi cartera.

Con montones de billetes de dólar en el banco, hay un riesgo de que dos pudieran tener por casualidad el mismo número, o que alguien pueda inventarse números y pagar con ellos con la esperanza de que los números que invente concuerden, por casualidad, con los números asociados con billetes en el banco. Pero ambos problemas se vuelven insignificantes si, en lugar de usar números de cinco dígitos usamos números de cien dígitos. La posibilidad de que dos números aleatorios de cien dígitos resulte ser la misma es mucho menor que la posibilidad

de que al pagador, beneficiario y al banco les caiga un rayo al mismo tiempo.

Mecánica robótica

Se te podría haber ocurrido que si tienes que escribir un número aleatorio de cien dígitos siempre que quieras comprar un dólar de dinero electrónico del banco y dos más cada vez que recibas uno de otro, por no mencionar mandar un correo electrónico anónimo al banco por cada dólar que recibas, el dinero electrónico podría acarrear más molestias de lo que vale. No te preocupes: ese es el trabajo de tu ordenador, no tuyo. Con un sistema de dinero electrónico competentemente diseñado, el programa se ocupa de todos los detalles matemáticos; solo tienes que preocuparte de tener bastante dinero para pagar las deudas (virtuales). Le dices a tu ordenador qué pagar a quién; te dice qué otra gente te ha pagado y cuánto dinero tienes. Los números aleatorios, comprobaciones de firmas digitales, firmas ciegas y todo lo demás se hace en un segundo plano. Si te resulta difícil creerlo, piensa en lo poco que sabemos la mayoría de nosotros de cómo funcionan las herramientas que utilizamos rutinariamente, como coches, ordenadores o radios.

DINERO ELECTRÓNICO Y PRIVACIDAD

Cuando a Chaum se le ocurrió la idea del dinero electrónico, el correo electrónico no era lo bastante popular para hacer del *spam* un problema. Lo que le motivó fue el problema que discutimos en el capítulo 4: la pérdida de privacidad creada por la capacidad del procesamiento de información moderno para combinar información disponible públicamente para dar lugar a un retrato detallado de cada individuo.

Piensa en una aplicación del dinero electrónico en la que Chaum ha seguido trabajando: recaudación de peaje automatizada. Sería muy cómodo si, en vez de parar en un peaje cuando entremos o salgamos de

la autopista de pago, pudiéramos simplemente pasarla, haciendo el pago automáticamente en forma de comunicación inalámbrica entre el peaje(sin personas) y el coche. La tecnología para hacerlo existe y hace mucho que se ha usado para proporcionar recolección de peajes automatizado para autobuses en algunas carreteras.

Un problema es la privacidad. Si el pago se realiza con tarjeta de crédito, o si la agencia de peaje suma los peajes de cada mes y te manda una factura, alguien tiene un registro completo de cada viaje que has hecho por autopista de peaje cada vez que cruzas un control. Si lidiamos con la contaminación de los vehículos midiendo los humos de los escapes de los vehículos que pasan y multando a sus dueños, alguien acaba con registros detallados, si bien algo fragmentados, de dónde estabas en qué momento.

El dinero electrónico soluciona ese problema. Mientras pasas el peaje, tu coche paga cincuenta céntimos en dinero electrónico anónimo. Para cuando hayas recorrido unos metros por la carretera, el peaje (en línea) ha comprobado que el dinero es correcto; si no lo es, salta una alarma, se activa una cámara, y, si no paras, acabará apareciendo un policía de tráfico en tu busca. Pero si el dinero es correcto, puedes ir tranquilamente a hacer tus cosas, y no hay registro del paso por el peaje. La información nunca existió, salvo en tu cabeza. Algo similar ocurre con los cobros del sistema de contaminación automatizado.

También funciona con las compras. El dinero electrónico (esta vez codificado en una pequeña tarjeta en tu cartera, un ordenador de mano en el bolsillo, o quizás incluso un pequeño chip bajo la piel) podría proporcionar muchas de las comodidades de una tarjeta de crédito con el anonimato del dinero. Si quieres que el vendedor sepa quién eres, eres libre de decírselo. Pero si prefieres mantener tus transacciones en privado, puedes.

DINERO PRIVADO: UNA NUEVA VIEJA HISTORIA

Hasta ahora, mis ejemplos han dado por hecho que el dinero electrónico se producirá y lo pagarán los bancos privados, pero

denominados en dinero del Gobierno. Ambos son probables, al menos a corto plazo. Ninguno es necesario.

El dinero privado denominado en dólares ya es común. Mi fondo de mercado monetario se encuentra denominado en dólares, aunque Merrill Lynch en verdad no tiene una pila de billetes en una cámara que corresponda a la cantidad de dinero «en» mi cuenta. Mi carnet universitario hace las veces de tarjeta, con alguna cantidad de dólares almacenada en su banda magnética, una cantidad que desciende cada vez que uso la tarjeta para comprar comida en el campus. Un banco podría emitir dinero electrónico sobre la misma base. Cada dólar de dinero electrónico representa un derecho a recibir un billete de dólar. Los activos reales que apoyan ese derecho consisten no en una pila de billetes, sino en *stock*, bonos y similares, que tienen la ventaja de pagar interés al banco siempre que el dólar de dinero electrónico esté circulando ahí fuera.

Mientras que no tengo que saber nada sobre ti para aceptar tu dinero electrónico, sí tengo que saber algo sobre el banco que lo emite, lo suficiente para asegurarme de que me acabará pagando el dinero. Ello significa que cualquier dinero electrónico que se espere que circule globalmente lo emitirán organizaciones con reputación. En un mundo de transmisión de información casi instantánea, esas organizaciones tendrán un fuerte incentivo para mantener sus reputaciones, ya que una falta de confianza acabará en que los que tienen el dinero traigan los billetes virtuales para cobrarlos, eliminando la fuente de ingresos que proporcionaban los activos que apoyaban a esos billetes.

Algunos economistas, rechazando la idea del dinero privado, han argumentado que una institución así es inherentemente inflacionaria. Puesto que emitir dinero no cuesta nada al banco y le da el interés sobre los activos que compra con el dinero, siempre interesa al banco emitir más. La refutación de este argumento particular se publicó en 1776. Cuando Adam Smith escribió *La riqueza de las naciones*, el dinero de Escocia consistía sobre todo en billetes emitidos por bancos privados, pagables en plata[36]. Como apuntó Smith, aunque que un banco podría imprimir tantos billetes como desee, no puede persuadir a otra gente de que tengan un número ilimitado de sus billetes. Un

[36] White, 1995.

cliente que tienen mil dólares en dinero virtual (o billetes escoceses) cuando solo necesita cien está renunciando al interés que podría estar ganando si tuviera en cambio los otros novecientos en algún activo que genere interés. Es una buena razón para limitar su tenencia en efectivo a la cantidad que necesita para las transacciones del día a día.

¿Qué sucede si un banco intenta emitir más dinero del que la gente desea tener? El exceso vuelve a pagarse. El banco está malgastando sus recursos imprimiendo dinero, intentando ponerlo en circulación, solo para que se devuelva cada billete de más de inmediato por dinero en efectivo (en el caso de Smith, plata). La obligación del banco de pagar su dinero garantiza su valor, y a ese valor hay una cantidad fija de dinero que la gente elegirá tener.

Supongamos que todo el dinero en papel de un banco particular, que la circulación del país puede emplear y absorber fácilmente, asciende exactamente a cuarenta mil libras; y que para responder a demandas ocasionales, este banco está obligado a mantener en todo momento en sus fondos diez mil libras en oro y plata. Si este banco intenta hacer circular cuarenta y cuatro mil libras, las cuatro mil que se encuentran por encima de lo que la circulación puede emplear y absorber fácilmente regresarán al banco casi tan rápido como se emitieron.

(*Riqueza de las naciones*, Libro I, capítulo 2)

Hasta ahora hemos dado por hecho que el dinero electrónico futuro se denominará en dólares. Los dólares tienen una gran ventaja: proporcionan una unidad común ya de uso extendido. También tienen una gran desventaja: los produce un Gobierno, y podría ser que no siempre interesara a ese Gobierno mantener su valor estable, o incluso predecible. Según las pruebas del pasado, los Gobiernos a veces incrementan o disminuyen el valor de su moneda, por descuido o por cualquier propósito político. En el caso extremo de hiperinflación, un Gobierno intenta financiar sus actividades con la prensa, incrementando rápidamente la cantidad de dinero y rebajando su valor. En casos menos extremos, un Gobierno podría provocar inflación para beneficiar a los deudores bajando el valor real de sus deudas (los Gobiernos mismos son a menudo deudores, de ahí los beneficios

potenciales de una política así), o podrían provocar inflación o deflación en el proceso de intentar manipular su economía con fines políticos.

Los dólares tienen una segunda desventaja, aunque quizás menos seria. Ya que los emite un Gobierno determinado, los ciudadanos de otros Gobiernos podrían preferir no usarlos. Esto no ha evitado que los dólares se conviertan en una moneda mundial *de facto*, pero es una razón por la que una moneda nacional podría no ser el mejor estándar en el que basar el dinero electrónico. La alternativa más simple sería un estándar de mercancía, asignando como unidad de dinero electrónico un gramo de plata u oro o alguna otra mercancía con la que se comercie de forma global.

Bajo un estándar de mercancía así la unidad monetaria, si bien ya no se encuentra bajo el control de un Gobierno, está sujeta en cambio a las fuerzas que afectan al valor de la mercancía particular en que está basada. Si se descubren grandes cantidades de oro o si alguien inventa técnicas nuevas y mejores de extraer oro de menas con baja concentración, el valor del oro, y de la moneda basada en oro, descenderá[37]. Si, por otro lado, se encuentran nuevos usos importantes del oro pero se extrae poco oro nuevo, el valor del oro subirá y los precios caerán. Así, la mercancía como moneda lleva consigo al menos algún riesgo de fluctuaciones impredecibles en su valor, y, por tanto, en los precios que se miden con ella.

El problema se soluciona reemplazando un estándar mercancía simple por un conjunto de mercancías. Trae un millón de dólares Friedman y estoy de acuerdo en darte a cambio diez onzas de oro, cuarenta de plata, la propiedad de mil fanegas, cada una de ellas de trigo de grado 1 y soja de grado 2, una tonelada de acero inoxidable de grado S30040… Si el poder adquisitivo de un millón de dólares es menor que el valor de ese conjunto, es rentable que la gente reúna un millón de dólares Friedman, los intercambie por el conjunto y venda sus contenidos, con

---

[37] El ejemplo no es completamente imaginario. A finales del siglo XIX, el efecto combinado del descubrimiento de los campos de oro de Sudáfrica y la invención del proceso de cianuro para extraer oro de mena de baja calidad llevó a una inflación del oro, aunque leve comparada con las inflaciones de dinero fiduciario. En el siglo XVISe produjo una inflación anterior de oro (y plata) por el flujo de entrada de ambos metales provenientes del Nuevo Mundo.

lo que me obligan a cumplir la promesa y, en el proceso, reducir la cantidad de mi moneda en circulación. Si el poder adquisitivo de mi moneda es más que el valor de las mercancías por las que se comercia, me interesa emitir más dinero. Ya que el conjunto contiene muchas mercancías distintas, se puede esperar que los cambios aleatorios en los precios de las mercancías se equilibren, con lo que obtenemos un estándar estable de valor.

Un conjunto de mercancías es una buena solución teórica al problema de los estándares monetarios, pero implementarlo tiene una seria dificultad práctica: conseguir que todas las firmas que emitan dinero electrónico estén de acuerdo en el mismo conjunto. Si no consiguen establecer un estándar común, acabamos en un ciberespacio en que gente diferente utilice distintas monedas y las tasas de intercambio entre ellas varíen aleatoriamente.

No es una situación que no pueda funcionar (los europeos vivieron así durante mucho tiempo), pero es molesto. La vida es más sencilla si la moneda que utilizo es la misma que la de la gente con la que hago negocios. Nuestro sistema mundial del presente (múltiples monedas del Gobierno, cada una con casi un monopolio en el territorio del Gobierno que las emite) está construido sobre ese hecho. Funciona porque la mayoría de las transacciones se realizan con la gente cercana a ti y ellos probablemente viven en el mismo país. Funciona menos bien en Europa que en Norteamérica porque los países son más pequeños, y por ello los países europeos han cambiado, en su mayoría, sus monedas nacionales al euro.

Un sistema de múltiples monedas monopolizadas por el Gobierno funciona menos bien en el ciberespacio porque ahí las fronteras nacionales son transparentes. Para transacciones de información, la geografía es irrelevante: puedo descargar *software* o imágenes digitales desde Londres tan fácilmente como desde Nueva York. Para las compras de objetos físicos en línea, la geografía no es completamente irrelevante, ya que los bienes tienen que ser entregados, pero es menos relevante que en las compras en el espacio real. Con un sistema de monedas nacionales, todo el mundo del ciberespacio tiene que hacer malabares con múltiples monedas en el proceso de descubrir cuál es el mejor precio y pagarlo. La solución obvia es establecer un solo estándar

de valor, adoptando una moneda nacional (probablemente, el dólar, posiblemente, el euro), o estableciendo un estándar privado como el tipo de conjunto de mercancías descrito anteriormente.

Podría no ser la única solución. La razón por la que todos quieren usar la misma moneda que sus vecinos es que la conversión de monedas es una molestia. Pero esta conversión es aritmética y los ordenadores lo hacen rápido y barato. Quizás, con algunas mejoras menores en las interfaces en que hacemos negocios en línea, podríamos hacer irrelevante la elección de moneda, permitiendo que coexistan estándares múltiples.

Vivo en EE.UU.; tú vives en la India. Tienes bienes para vender, mostrados en una página web, con los precios en rupias. Veo esa página por mi nuevo navegador: Firefox versión 9.0. Una característica del nuevo navegador es que es transparente monetariamente. Publicas los precios en rupias, pero lo veo en dólares. El navegador realiza la conversión al vuelo, usando tasas de intercambio que lee, minuto a minuto, de la página web de mi banco. Si quiero comprar tus mercancías, pago en dinero electrónico denominado en dólares; mi navegador lo manda a mi banco, que te manda dinero electrónico denominado en rupias. Ni sé, ni me importa, en qué país estás o qué monedas usas: todo es dólares para mí.

La transparencia monetaria será más sencilla en línea, donde todo se filtra por navegadores de todas formas. Uno puede imaginar, con un poco más de esfuerzo, equivalentes en el espacio real. Una discreta etiqueta en mi solapa me proporciona mi moneda preferida; una etiqueta de precios automatizada en el estante de la tienda lee mi etiqueta y muestra el precio en consecuencia. Si no, el precio se muestra en una etiqueta de precio muda, leída por una videocámara inteligente situada en la montura de mis gafas, convertido por mi ordenador de bolsillo y escrito en el aire por la pantalla de visualización frontal generada por las gafas.

Mientras escribo, los países de Europa se encuentran en los estadios finales de reemplazar sus múltiples monedas nacionales por el euro. Si el marco que he presentado resulta ser correcto, podrían haber conseguido una moneda común justo cuando se volvía innecesario.

Ahora tenemos tres posibilidades para el dinero electrónico. Podría producirse por medio de múltiples emisores, pero denominado en dólares o en cualquier otra moneda nacional de uso extendido. Podría denominarse en algún estándar de valor común no gubernamental (oro, plata o un conjunto de mercancías). Podría denominarse en una variedad de estándares distintos, quizás incluyendo tanto monedas nacionales como mercancías, con una conversión realizada transparentemente, de forma que todo individuo vea un mundo en que todos usan su dinero. Todas esas formas de dinero electrónico podrían producirlas empresas privadas, probablemente bancos, o Gobiernos[38].

¿SUCEDERÁ?

Durante la Segunda Guerra Mundial, George Orwell escribió artículos regulares para la *Partisan Review*, una revista estadounidense. Hacia el final de la guerra, escribió una retrospectiva en la que discutía en qué había acertado y en qué había fallado[39]. Una de sus conclusiones fue que, por lo general, tenía razón en la forma en que el mundo se estaba moviendo, se equivocó en lo que tardaría en llegar allí. Vio correctamente el patrón lógico, pero no consiguió tener en cuenta la enorme inercia de la sociedad humana.

Algo similar pasa aquí. Los artículos de David Chaum que dibujan la base para un dinero electrónico completamente anónimo se publicaron en diarios técnicos en la década de los 80 y se resumieron en un artículo de 1992 en *Scientific American*. Desde entonces, varias personas, entre las que me encuentro yo, han estado prediciendo el alza del dinero electrónico siguiendo la línea que él trazó. Mientras que las piezas de su visión se han vuelto reales en otros contextos, todavía no hay nada cercano a un dinero electrónico completamente anónimo para uso general. El mismo Chaum, trabajando con el banco Mark Twain Bank en Saint Louis, intentó conseguir un dinero electrónico semianónimo

[38] Para un producto actual que sigue estas líneas, véase http://www.e-gold.com. Que yo sepa, su dinero no es dinero electrónico anónimo, sino que está organizado de tal forma que tu tenencia se defina en oro, pero los pagos se pueden convertir en toda una variedad de monedas.

[39] "London Letter to Partisan Review," en Orwell, 1968.

en circulación, uno que permitiera a una parte hacer una transacción que se identificara por la acción conjunta de la otra parte y el banco. El esfuerzo falló y se abandonó.

Otra razón por la que no ha sucedido es que el comercio en línea se ha vuelto lo bastante grande como para justificarlo solo recientemente. Una segunda razón que sospecho pero no puedo probar es que los Gobiernos nacionales no están contentos con la idea de un dinero usado globalmente que no puedan controlar y, por tanto, son reacios a permitir que bancos privados (muy regulados) creen tal dinero. Una tercera razón, muy relacionada con las anteriores, es que un dinero electrónico verdaderamente anónimo eliminaría una forma rentable de ejecutar la ley. No hay una forma práctica de ejecutar las leyes de blanqueo de dinero una vez sea posible mover arbitrariamente grandes cantidades de dinero a cualquier parte del mundo, sin rastro, con un click. La razón final es que el dinero electrónico solo me resulta útil si mucha otra gente lo está usando, lo que plantea el problema de arrancarlo.

Estos hechos han demorado la introducción del dinero electrónico. No pienso que lo vayan a parar. Solo se necesita un país dispuesto a permitirlo y una institución emisora en ese país dispuesta a emitirlo para que exista el dinero electrónico. Una vez exista, será políticamente difícil que otros países prohíban a sus ciudadanos usarlo y casi imposible, si se prohíbe, ejecutar la prohibición. Hay muchos países del mundo, incluso si nos limitamos a aquellos con instituciones lo suficientemente estables para que la gente de otras partes confíen en su dinero. Por tanto, mi mejor suposición es que alguna versión de una de las monedas que he descrito en este capítulo existirá en algún momento de la siguiente década o así.

SIETE

CONTRATOS EN EL CIBERESPACIO

Contratas a alguien para arreglar el tejado e, imprudentemente, le pagas por adelantado. Dos semanas más tarde, le llamas para preguntar cuándo va a terminar el trabajo. Tras tres meses de alternar promesas con silencios, lo demandas, probablemente por proceso moritorio.

Denunciar a alguien es una molestia, por eso has esperado tres meses. En el ciberespacio será todavía más molesto. La ley que se aplica a una disputa depende, de forma enrevesada, de dónde viven las partes y dónde sucedieron los eventos del litigio. Un contrato realizado en línea no tiene una localización geográfica y la otra parte podría vivir en cualquier parte del mundo. Demandar a alguien en otro estado federado ya es lo bastante difícil; denunciar a alguien de otro país es mejor dejarlo para profesionales, que no son baratos. Si, como sugerí en un capítulo anterior, el uso de la encriptación en línea lleva a un mundo de privacidad férrea, en el que mucha gente hace negocios sin revelar su identidad en el espacio real, la ejecución legal de contratos se vuelve no meramente difícil, sino imposible. No hay forma de demandar a alguien si no sabes dónde está.

Sin embargo, incluso en nuestras vidas en el espacio real, hay otra manera de ejecutar los contratos, y una que es probablemente más importante que el litigio. La razón por la que los grandes almacenes hacen bien con sus promesas de «*money back, no questions asked*» («dinero devuelto, sin preguntas»), y la razón por la que la gente que me poda el césped sigue haciéndolo una vez a la semana incluso cuando estoy fuera de la ciudad y no puedo pagarles no es el sistema judicial. Es improbable que los clientes demanden a unos grandes almacenes, por muy irrazonables que sean sus razones para negarse a devolver algo, y es improbable que la gente que poda mi césped me denuncien, incluso si me niego a pagarles por sus últimas tres semanas de trabajo.

Lo que ejecuta un contrato en ambos casos es la reputación. Los grandes almacenes quieren mantenerme como cliente y no lo harán si llego a la conclusión de que no se puede confiar en ellos. No solo me

perderán, podrían también perder a algunos de mis amigos, a los que es esperable que me queje. La gente que poda mi césped hace un buen trabajo a un precio razonable, gente así no es fácil de encontrar y sería estúpido ofenderles al negarme a pagarles por su trabajo.

Cuando cambiamos nuestras transacciones del vecindario a Internet, la ejecución legal se vuelve más difícil. Sin embargo, la ejecución basada en la reputación se vuelve más sencilla. La red proporciona un magnífico conjunto de herramientas para recopilar y diseminar información, incluida aquella acerca de en quién y en quién no se puede confiar.

En un nivel informal, esto sucede de forma rutinaria tanto por Usenet como por la Web. Hace algunos años, oí que mi ordenador de mano favorito (un ordenador con todas las características, completo con teclado, procesador de texto, hoja de cálculo y mucho más, que cabía en mi bolsillo y estaba en funcionamiento más o menos siempre gracias a su batería recargable) se encontraba disponible a un precio absurdamente bajo en una reventa de descuento, aparentemente porque el intento de venderlo en el mercado estadounidense[40] había fallado y la compañía que lo intentó estaba deshaciéndose de su *stock* del rebautizado como Psion Revos (también conocido como Diamond Makos). Fui a la Web, busqué al distribuidor de la reventa, y en el proceso descubrí que se le había acusado de no conseguir mantener sus garantías de servicio y actualmente se encontraba en problemas con las autoridades de varios estados federados. El mismo proceso funciona de una manera algo más organizada a través de páginas web especialistas: MacInTouch para los usuarios de Macintosh, la Digital Camera Resource Page para clientes de cámaras digitales, y muchos más.

Para una versión diferente de ejecución basada en la reputación en línea, piensa en eBay. No vende bienes: vende el servicio de ayudar a otra gente a vender bienes, por medio de un sistema de subasta en línea. Esto plantea un problema obvio. Los vendedores podrían estar localizados en cualquier parte, a menudo fuera de los Estados Unidos.

[40] http://www.psion.com/, http://www.psioninc.com/. Por desgracia, Psion ha abandonado ahora el mercado del consumidor. Si tan solo dieran la licencia a Sony o Nokia del hechizo mágico que hizo posible que ellos, y solo ellos, construyeran un teclado utilizable en un ordenador de bolsillo o, mejor aún, en un *smartphone*, podría tener la máquina de mi sueños.

La mayoría de las transacciones, aunque no todas, tienen que ver con bienes de valor modesto, así que demandar por fallo de envío, especialmente a alguien de fuera de EE.UU., rara vez es una opción práctica. Con millones de compradores y vendedores, no es probable que cada comprador individual compre muchas cosas de un vendedor particular, así que el vendedor necesita preocuparse solo levemente de su reputación con ese comprador particular. ¿Por qué no cogen el dinero todos los vendedores y sencillamente salen corriendo?

Una razón es que eBay proporciona un apoyo extensivo para la ejecución reputacional. Siempre que ganes una subasta de eBay tienes la opción, tras recibir el envío, de informar de tu evaluación de la transacción —si los bienes eran como estaban descritos y se enviaron en buenas condiciones, y cualquier otra cosa que quieras añadir—. Siempre que pujas en eBay, tienes acceso a todos los comentarios anteriores sobre el vendedor, tanto resumidos como, si estás lo bastante interesado, al completo. Los vendedores exitosos de eBay tienen por lo general un registro con muchos comentarios, muy pocos de ellos negativos.

Por supuesto, hay maneras de que un villano lo bastante emprendedor pueda intentar vencer al sistema. Una podría ser montar una serie de subastas falsas, vendiendo algo bajo un nombre, comprándolo con otro y dándose una buena crítica. Al final construye una cadena de críticas brillantes y las utiliza para vender una docena de bienes no existentes a altos precios, pagaderos por adelantado.

Es posible, pero no es barato. Después de todo, eBay se llevará su parte de cada una de estas subastas falsas. Los compradores nominales necesitarán muchas identidades diferentes para que el truco no sea obvio, lo que implica costes adicionales. Mientras tanto, todo lo que tienen que hacer los vendedores legítimos para construir su reputación es un negocio honesto, como siempre. En cuanto a eBay mismo, para mantener su reputación como un buen sitio para comprar y vender, intenta de varias formas evitar que los compradores y vendedores abusen de los mecanismos de reputación que ha creado. Estoy seguro, partiendo de que no tengo información de dentro, que al menos un villano lo ha conseguido, pero no parece ser suficiente para desanimar seriamente a la gente de que usen eBay.

Otra manera de que un vendedor deshonesto pudiera intentar aprovecharse del sistema es comprando bienes de los competidores con nombre falso y luego publicar información negativa (falsa) sobre la transacción. Podría valer la pena en un mercado con solo unos pocos vendedores, y, que yo sepa, ha sucedido. Pero en el típico mercado de eBay, con muchos vendedores y compradores, difamar a un competidor simplemente transfiere el negocio a otro.

LA LÓGICA DE LA EJECUCIÓN REPUTACIONAL

Mientras que la ejecución de la reputación siguiendo las líneas de lo que proporciona actualmente eBay es adecuada para muchos fines, sería útil tener sistemas que sean más difíciles de engañar. Antes de mirar cómo podrían funcionar, merece la pena pensar un poco más sobre la lógica de la ejecución de la reputación. El derecho penal y el derecho de responsabilidad civil existen, en gran parte, como formas de castigar el mal comportamiento. En el caso de la ejecución de la reputación, en cambio, el castigo es solo una consecuencia indirecta de acciones realizadas por otras razones. Piensa en un ejemplo (imaginario):

Las noticias de que Charley compró una chaqueta cara en los grandes almacenes locales, su mujer le hizo devolverla y se negaron a devolverme el dinero no me proporciona una razón para querer castigar a la tienda. Desde que Charley me contó lo que pensaba de verdad de mi último libro, he considerado sus desgracias como lo que se merece. A medida que la noticia se expande, cada vez más gente para de comprar en esa tienda en particular. La razón no es que queramos castigarles: el hábito desafortunado de Charley de decirle a la gente lo que piensa de verdad le ha dejado con pocos amigos. La razón es protegernos. También algún día podremos comprar algo que nuestras esposas no aprueben.

La ejecución de la reputación funciona difundiendo información verdadera sobre un mal comportamiento. La gente que recibe esa información modifica sus acciones en consecuencia, lo que impone

costes sobre los que se comportaron mal[41]. Como muestra este ejemplo, algo que determina lo bien que funciona la ejecución de la reputación es la capacidad de que las terceras partes interesadas obtengan información sobre quién engañó a quién.

Para verlo, supón que cambiamos un poco la historia haciendo que no es que Charley simplemente no tenga tacto, sino que es deshonesto por rutina. Ahora, cuando se queja de que la tienda se negó a coger la chaqueta aunque estuviera en buenas condiciones, deducimos que su idea de buenas condiciones probablemente incluía múltiples manchas de tinta y una manga de menos, debido a la reacción de su esposa a cómo ha estado gastando su dinero (también la conocemos a ella) y seguimos siendo clientes de la tienda.

Una razón por la que los costes de la información son importantes es que si las terceras partes interesadas no saben quién tiene la culpa, no saben con quién evitar las futuras transacciones. Una razón más sutil es que si las terceras partes no pueden descubrir fácilmente quién tiene la culpa en una disputa, la disputa puede no hacerse pública jamás. Si te acuso de estafarme, lo negarás, por supuesto. Las terceras partes razonables, incapaces de comprobar las afirmaciones de cualquiera de las partes, deducen que uno de nosotros es un impresentable. No tienen manera de descubrir quién, y, por tanto, es prudente evitar a ambos. Anticipándome a ese resultado, decido tragarme mis pérdidas e intentar ser más cuidadoso la próxima vez; quejarme solo empeorará las cosas[42]. Así que la ejecución de la reputación requiere un marco que facilite que las terceras partes interesadas determinen quién tiene la culpa.

Ese marco existe y se usa para zanjar las disputas dentro de la industria en muchas industrias diferentes. Se llama *mediación*.

Tú y yo llegamos a un acuerdo y especificamos el mediador privado que zanjará nuestros desacuerdos sobre los términos. Tiene lugar un desacuerdo: exiges mediación. El mediador arbitra a tu favor. Si te niegas a obedecer el fallo, el mediador puede hacerlo público. Una

---

[41] Para una discusión en extenso sobre la ejecución reputacional, véase Klein, 1997.

[42] Este problema es, aparentemente, responsable de los recientes cambios en la política de retroalimentación de eBay; se disuadía a los compradores de que dejaran mensajes negativos sobre los vendedores por preocupación por que los vendedores contraatacaran de la misma manera.http://pages.ebay.com/services/forum/new.html.

tercera parte interesada, típicamente otra empresa en la misma industria, no tiene que conocer los hechos de la disputa para saber quién tiene la culpa. Todo cuanto tiene que saber es que ambos acordasteis el mediador y él dice que he incumplido el acuerdo[43].

Esto funciona bien en una industria porque la gente que se ve involucrada conoce a los demás y están familiarizados con las instituciones de la industria para zanjar disputas. Funciona menos bien para las disputas entre una firma y uno de sus muchos clientes. Es improbable que otros clientes, a menos que también sean parte de la industria, sepan lo bastante de las instituciones para tener seguridad en quién engañaba a quién. ¿Y en el ciberespacio?

Muy cercano a cero: los costes de la tercera parte en el ciberespacio

Tú y yo acordamos un contrato en línea. El contrato contiene el nombre del mediador que resolverá las disputas y su clave pública (la información necesaria para comprobar su firma digital). Ambos firmamos digitalmente el contrato y cada uno se queda una copia.

Surge una disputa: me acusas de no cumplir mi acuerdo y exiges mediación. El mediador arbitra a tu favor y me ordena pagarte cinco mil dólares en daños. Me niego. El mediador escribe un informe de cómo acabó el caso: exigió indemnización por daños y perjuicios, me negué a pagarlos. Lo firma digitalmente y te manda una copia.

Ahora tienes el contrato original y el veredicto del mediador. Mi firma digital en el contrato original demuestra que accedí a ese mediador; su firma digital en el veredicto prueba que incumplí ese acuerdo. Esa es toda la información que una tercera parte interesada necesita para deducir que no se debe confiar en mí.

Pones ambas cosas en una página web, con mi nombre por todas partes para los motores de búsqueda que busquen información sobre mí, y escribes la URL a cualquiera que creas que podría querer realizar negocios conmigo en el futuro. Cualquiera que acceda a la página

---

[43] Los interesados en algo más allá de esta enumeración altamente estilizada podrían desear echar un vistazo al trabajo de Lisa Bernstein sobre el arbitraje en http://www.law.uchicago.edu/faculty/bernstein/publications.html.

puede comprobar los hechos —de forma más precisa, su ordenador puede comprobar los hechos comprobando las firmas electrónicas— en menos de un segundo. Habiéndolo hecho, sabe que soy el que incumplió el acuerdo. La explicación más probable es que soy deshonesto. Una posibilidad alternativa es que era lo bastante estúpido como para acordar un mediador sinvergüenza, pero probablemente tampoco quiere hacer negocios con estúpidos. Así, la tecnología de las firmas electrónicas hace posible la reducción de los costes de información a las terceras partes hasta casi cero, posibilitando la ejecución de la reputación efectiva en línea[44].

La ejecución privada de los contratos en esa línea soluciona los problemas planteados por el hecho de que el ciberespacio alarga muchas jurisdicciones geográficas. La ley relevante viene definida no por la jurisdicción, sino por el mediador privado elegido por las partes. Con el tiempo, podríamos esperar que se desarrollaran uno o dos cuerpos de normas legales en lo que respecta a los contratos, como se desarrolló históricamente la Ley Mercante, con muchos mediadores diferentes o empresas de mediadores que adopten las mismas normas legales, o similares[45]. Las partes contrayentes podrían entonces elegir mediadores según la reputación.

Para las transacciones a pequeña escala, simplemente proporcionas al navegador una lista de empresas de mediadores aceptables; cuando realices negocios con otra parte, el *software* selecciona un mediador de la intersección de las dos listas. Si no hay un mediador aceptable para ambas partes, el *software* os lo notifica y os hacéis cargo. Para transacciones mayores, la posibilidad de mediador es una de las cosas que los humanos que negocian el contrato pueden discutir.

La ejecución privada también resuelve el problema de ejecutar contratos cuando al menos una de las partes es, y desea seguir siendo, anónima. Las firmas digitales hacen posible combinar anonimato con

---

[44] Los costes de la mediación, por supuesto, no son nulos. Pero los paga la gente que firmó el contrato, no las terceras partes interesadas.

[45] Como afirmó Bruce Benson, la forma en que la Lex Mercatoria se desarrolló en la temprana Edad Media era mediante un proceso así. También era un sistema de ley privada ejecutada mediante penas de reputación en un ambiente en que la ley estatal era inadecuada para la ejecución de contratos, en parte debido a la diversidad legal entre jurisdicciones. Véase Benson, 1998, "Evolution of Commercial Law" y "Law Merchant."

reputación. Un programador que vive en Rusia o Irak, donde el anonimato es la única forma de proteger los ingresos de los bandidos públicos o privados, tiene una identidad en línea definida por su clave pública; cualquier mensaje firmado por esa clave pública es suyo. Esa identidad tiene una reputación, desarrollada por las transacciones en línea pasadas. Cuantas más veces haya demostrado el programador que es honesto y competente, más gente estará dispuesta a contratarlo. La reputación es valiosa, así que el programador tiene un incentivo para mantenerla: manteniendo sus contratos[46].

El mercado de la reputación

(En la Tierra) incluso tienen leyes para asuntos privados como contratos. En serio. Si la palabra de un hombre no sirve, ¿quién querría hacer negocios con él? ¿No tiene reputación?

Manny en *La luna es una cruel amante*, de Robert Heinlein

Hay una forma de que el mundo en línea que he estado describiendo haga más difícil la ejecución de contratos que en el mundo real. En el mundo real, mi identidad está unida a un cuerpo físico, identificable por el rostro, huellas dactilares y similares. No tengo la opción, tras destruir mi reputación de honesto en el espacio real, de crear un nuevo yo, completo, con un rostro nuevo, nuevas huellas dactilares y una reputación intachable.

En línea sí tengo esa opción. Siempre que otra gente esté dispuesta a tratar con identidades en el ciberespacio no unidas a identidades del espacio real, tengo la opción de hacerme con una nueva pareja clave pública / clave privada y aparecer en línea con una nueva identidad y una reputación limpia.

Se sigue que la ejecución de la reputación solo funcionará con gente que tiene reputación: suficiente capital de reputación de forma que el coste de abandonar la identidad en línea actual y su reputación supere

[46] Una buena descripción ficticia de la combinación de anonimato con la reputación en línea se da pronto en Stiegler, 1999.

la ganancia de un solo acto de engaño. Alguien que quiere negociar anónimamente en una industria de mucha confianza tiene que comenzar pequeño, labrándose la reputación hasta el punto de que su valor sea suficiente para que sea racional confiar en él para transacciones más grandes. Lo mismo pasa hoy en día con las industrias en que la ejecución se lleve primariamente por medio de mecanismos de reputación[47].

El problema de crear nuevas identidades no se limita al ciberespacio. El equivalente en el espacio real de crear un nuevo par de claves es preparar nuevos papeles de incorporación. El revestimiento de mármol para edificios de bancos y caras campañas de publicidad pueden verse como maneras de que una nueva empresa publique un bono de reputación para persuadir a los que negocian con ella de que pueden confiar en ella de una forma que preserve su reputación. Las identidades del ciberespacio no tienen la opción del mármol, al menos si quieren seguir siendo anónimas, pero sí tienen la opción de invertir en una larga serie de transacciones o en otras actividades costosas, como la publicidad o la caridad bien publicitada, para establecer una reputación que se una a su futura actuación.

¿Qué pasa con las entidades (empresas o individuales) que no se involucran en negocios a largo plazo y que tampoco tienen una reputación valiosa ni están dispuestas a pagar para adquirir una? ¿Cómo van a garantizar su actuación contractual en este mundo?

Una solución es subirse a la reputación de otra entidad que sí. Supón que soy una identidad en línea anónima que está creando un contrato que después puede que me interese romper. ¿Cómo, sin tener reputación, persuado a la otra parte de que me ceñiré a mi palabra? ¿Qué evita que celebre el contrato, me ponga de acuerdo en un

---

[47] Stiegler, 1999, contiene una ilustración entretenida de este argumento. Un personaje central ha mantenido dos identidades en línea, una, con una buena reputación por transacciones legales y la otra, con una reputación deliberadamente turbia por transacciones cuasilegales como adquisiciones de propiedad robada. En un punto de la trama, su identidad buena se encuentra casi terminando una transacción honesta rentable cuando se le ocurre que sería incluso más rentable si, habiendo recaudado el pago de este trabajo, no consiguiera, en el último minuto, realizar la entrega. Descarta esa opción sobre la base de que tener una identidad con buena reputación le ha dado la oportunidad de una transacción rentable, y si destruye esa reputación pasará mucho tiempo hasta que consiga otras oportunidades así.

mediador, rompa el contrato, ignore el veredicto del mediador y me vaya con las ganancias, sin importarme el daño a mi reputación no existente?

Resuelvo el problema ofreciendo publicar una garantía de actuación con el mediador en moneda digital anónima. El mediador es libre de asignar todo o parte de la garantía a la otra parte como daños y perjuicios de la rotura. Esta solución (aprovecharse de una tercera parte con reputación) no es puramente hipotética. Los compradores de eBay ya pueden complementar la ejecución de la reputación directa con los servicios de un agente *escrow* o garante (una tercera parte de confianza que se queda con el pago del comprador hasta que los bienes se han inspeccionado y luego se los da al vendedor).

Esta solución depende todavía de la ejecución de la reputación, pero esta vez la reputación pertenece al mediador. Con todas esas partes anónimas, podría simplemente robar la garantía, pero si lo hace, es improbable que siga mucho tiempo en el negocio. Si estoy preocupado por esas posibilidades, puedo exigir que el mediador firme un contrato especificando un segundo mediador independiente para que se enfrente a los conflictos entre él y el primer mediador. Mi firma en ese acuerdo vale muy poco, ya que no está apoyada por ninguna reputación, pero la firma del primer mediador en un contrato que lo obliga a aceptar el juicio del segundo mediador está apoyada por la reputación del primer mediador.

Un problema que podría ocurrírsele a algunos lectores. Estoy identificado en línea solo por mi firma digital. Alguien que obtiene de alguna forma una copia de mi clave privada tiene un cheque en blanco contra mí, hasta el límite del valor de mi reputación: puede firmar contratos como si fuera yo, recoger pagos y entonces dejarme que cumpla los contratos o perder mi reputación.

La solución obvia a este problema es guardar mi clave privada. Otra solución parcial es un mecanismo para retirar claves comprometidas, quizás un sitio web que mande correos para gente cuyas claves han resultado comprometidas, anunciando que ya no serán responsables de los contratos firmados con esa clave. Cuando me cree una reputación, puedo anunciar explícitamente que mi firma solo es válida para las

obligaciones hasta cierto límite, o durante un tiempo fijo de tiempo, con algún mecanismo explicado para renovarlo.

CONCLUSIÓN

Si los argumentos que he ofrecido son correctos, podemos esperar que el auge del comercio electrónico produzca un cambio sustancial hacia la ley privada ejecutada por los mecanismos reputacionales de forma privada. Mientras que el cambio debería de ser más fuerte en el ciberespacio, debería tener también un eco en el espacio real. Las firmas digitales reducen los costes de la información para las terceras partes interesadas, sucedan en línea las transacciones que se contratan o no. Y la existencia de un cuerpo de mediadores de confianza en línea hará la contratación de mediación privada por adelantado más familiar y más sencilla la confianza en la mediación privada para las transacciones, tanto en el espacio real como en el ciberespacio.

El uso de ejecución reputacional como una alternativa a la ejecución legal de contratos no es nada nuevo; existen múltiples ejemplos históricos. En este respecto, así como en varios discutidos después, el futuro podría parecerse más al pasado que al presente.

Los precios relativos rigen el mundo

Cuando era pequeño, uno de mis adultos favoritos era una amiga de mis padres llamada Dorothy Brady. Una razón era su hábito de traer pequeños regalos para mi hermana y para mí cuando venía de visita. Otra más importante era que siempre hacía cosas interesantes.

Uno de los proyectos tenía que ver con máquinas de pelar manzanas, los dispositivos en los que metes una manzana, giras una manivela y, si todo va bien, acabas con una manzana pelada, deshuesada e incluso, a veces, troceada. La conclusión de su investigación (realizada mediante la exploración de museos de Nueva Inglaterra) era que durante un periodo de unos doscientos años el diseño seguía siendo igual, pero los

materiales habían cambiado. Cuanto más atrás te remontabas, más parte de la máquina estaba hecha de madera y menos de metal.

En la vida real, Dorothy era una historiadora económica. Además de darle una excusa para curiosear los museos, su investigación proporcionaba un ejemplo de un patrón muy común en la historia económica. Cómo se hacen las cosas depende de los costes relativos de las alternativas. Cuando el metal es caro, y la madera y la mano de obra para trabajarla es barata, las cosas se hacen sobre todo de madera, y se usa el metal solo donde es esencial. A medida que el acero se hace cada vez menos caro en relación a la madera y la mano de obra, se usa cada vez más.

Este capítulo es sobre un ejemplo más nuevo de la misma lógica. La tecnología de Internet reduce el coste de hacer negocios con gente que está lejos, así que hacemos más. Por cuestión de práctica, solía comprar cosas solo de Inglaterra cuando estaba en Inglaterra. Hoy en día, comprar un libro de Inglaterra solo acarrea más problemas de forma marginal que comprarlo de la librería Barnes & Noble local. Rutinariamente, hacer negocios con la gente que está lejos aumenta los costes de zanjar disputas usando el sistema judicial del Gobierno, puesto que la jurisdicción de los tribunales se basa en gran parte en la geografía.

La tecnología de comunicaciones moderna hace mucho más fácil de lo que solía ser compartir información, y la tecnología de encriptación, en forma de firmas digitales, hace lo mismo verificando la información compartida. Ya no tienes que comprobar la parcialidad y reputación de tu informante o estudiar las pruebas para asegurarte de que nadie las ha retocado. Un cálculo te dice que un veredicto vino del mediador del que dice que viene; otro más te dice que ese mediador fue el que accedí a aceptar. Accedí a aceptar su veredicto, dice que incumplí ese acuerdo, caso cerrado.

Los tribunales del Gobierno y la reputación privada son formas alternativas de conseguir el mismo objetivo: hacer que la gente se ciña a su palabra. El coste de usar los tribunales del Gobierno ha subido. El coste de la información para las terceras partes interesadas (el ingrediente clave en la ejecución privada mediante la reputación) ha

bajado. El resultado predecible es un cambio que aleja de un medio y acerca al otro.

Encuentra un pelador de manzanas en un catálogo de utensilios de cocina. La manivela podría ser de madera o plástico. El resto será hierro.

OCHO

MARCAS DE AGUA Y ALAMBRE DE PÚAS

Los autores esperan que se les pague por su trabajo. También los programadores, músicos, directores de cine y mucha otra gente. Si no se les puede pagar por su trabajo, es probable que tengamos menos libros, películas, canciones, programas. Esto crea un problema si lo que se produce puede reproducirse de forma barata. Una vez esté ahí fuera, cualquiera que tenga una copia puede realizar otra, lo que hace que el precio de las copias baje hasta el coste de reproducirlas. La ley del *copyright* es un intento de resolver ese problema dando al creador de una obra el derecho legal de controlar la creación de copias. Lo bien que funcione depende de lo fácilmente que pueda ejecutarse ese derecho.

EL *COPYRIGHT* EN LOS MEDIOS DIGITALES

«Los rumores de mi muerte han sido exagerados sobremanera.»

Mark Twain. Quizás también el *copyright*. O quizás no.

Para ejecutar sus derechos legales, el propietario de un *copyright* tiene que ser capaz de descubrir que se copia ilegalmente y tomar acciones legales contra los responsables. Lo fácil que sea depende en gran parte de la tecnología del copiar.

Piensa en la prensa alrededor de 1910. Era grande y cara; imprimir un libro requería primero pasar cientos de páginas de impresión a mano. Eso hacía mucho menos caro imprimir diez mil copias de un libro en una prensa que cien copias en cien prensas diferentes. Ya que nadie quería diez mil copias de un libro para sí mismo, un productor tenía que encontrar clientes. Muchos clientes. Anunciando el libro, u ofreciendo su venta en librerías, llamaba la atención del propietario del *copyright*. Si no había autorizado la copia, podía localizar al pirata y demandarlo.

La ejecución se vuelve mucho más difícil si copiar es práctico en una escala de una o unas pocas copias (la situación actual de las obras digitales como programas informáticos, música digitalizada o películas en DVD). Los individuos que realizan una copia para ellos mismos o unas pocas para amigos son mucho más difíciles de localizar que los que realizan copias para un mercado masivo. Incluso si los localizas, es más difícil demandar a diez mil acusados que a uno. De ahí que, por motivos prácticos, las empresas limiten en su mayoría la ejecución de su*copyright* a la acción legal contra los infractores a gran escala.

La situación no es completamente desesperada desde el punto de vista del titular del *copyright*. Si el producto es un *software* usado en los negocios de forma global (Microsoft Word, por ejemplo), habrá organizaciones que usen no una copia, sino miles. Si eligen comprar uno y producir ellos mismos el resto, alguien podría darse cuenta y demandar.

Incluso si copiar se puede hacer a escala pequeña, queda el problema de la distribución. Si obtengo programas o canciones copiándolas ilegalmente de mis amigos, me limito a lo que poseen ellos, que podría no incluir lo que quiero. Podría preferir comprar de distribuidores que proporcionan un amplio rango de alternativas, y ellos, al ser objetivos potenciales de demandas de infringimiento, tienen un incentivo de comprar lo que venden legalmente más que producirlo ilegalmente. Así que incluso en un mundo en que se pueden copiar fácilmente muchas obras caras en formato digital (Word, por ejemplo), los productores de dichas obras todavía pueden usar la ley de *copyright* para que se les pague por lo que producen.

O quizás no. Como han demostrado Napster y luego sus sucesores *inter pares*, la distribución por Internet hace posible combinar la copia individual con la distribución para un mercado masivo, usando herramientas de búsqueda especialmente diseñadas para encontrar al individuo que resulta que tiene una canción en particular que quieres y está dispuesto a dejarte que la copies. Un sistema de distribución centralizado es vulnerable a ataques legales, como descubrió Napster. Pero desmantelar un sistema descentralizado como Gnutella o Freenet, que permite que los individuales de la red pongan disponibles para descarga sus colecciones de música a cambio

de poder descargar canciones de las colecciones de otra gente, es un problema más difícil. Si cada usuario copia una de tus canciones una vez, pero hay cien mil de ellos, ¿cómo puedes demandarlos a todos?

Quizás puedas, si te aprovechas adecuadamente de la tecnología. Un sistema descentralizado debe proporcionar alguna manera de encontrar a alguien que tenga la canción que quieres y esté dispuesto a compartirla. Los propietarios de *copyright* podrían usar el mismo *software* para localizar a los individuos que hacen que sus obras estén disponibles para copiarlas y demandarlos a todos, quizás en una demanda que una a muchos acusados. Puesto que la ley de *copyright* fija un mínimo de quinientos dólares por daños y perjuicios legales, denunciar a mil individuos, cada uno de los cuales ha realizado una copia de tu obra protegida por *copyright*, podría, en principio, proporcionar más dinero que denunciar a un individuo que había realizado diez mil copias.

Los intentos recientes en estas líneas generales llevados a cabo por la Asociación de Industria Discográfica de Estados Unidos (RIAA) han conseguido mucha publicidad, al menos parte de ella negativa. También se enfrentan a algunos problemas técnicos. Para empezar, según la ley actual, no está completamente claro cuándo son ilegales los intercambios de archivos no comerciales, aunque el Congreso podría cambiar esta situación, y probablemente los tribunales la harán[48]. También es difícil meter a múltiples acusados en una sola demanda, así que demandar a un número muy elevado puede ser caro. Por otra parte, si se espera que pierdan, uno podría no tener que ir muy lejos con la demanda antes de conseguir un acuerdo fuera de los tribunales. Y uno podría imaginarse modificaciones en las normas legales relevantes, quizás aplicables solo a demandas de *copyright*, que podrían hacer más sencilla la mecánica.

Aunque esta propuesta podría funcionar un tiempo, sus problemas a largo plazo deberían estar claros a partir de la anterior discusión sobre la privacidad férrea. Un sistema descentralizado bien diseñado localizaría a alguien dispuesto a dejarte copiar una canción, pero no dejaría que identificaras a la persona de la que la copiabas. No necesitas nombre, cara o número de la seguridad social para copiar el archivo que

[48] http://www.law.wayne.edu/litman/papers/read.htm.

contiene la canción que quieres, simplemente alguna forma de que los mensajes lleguen a y de él. Esto aumenta la posibilidad de que el deseo de la gente de descargar música sin pagar por ella o ser demandada pudiera ser el incentivo clave que nos empuje hacia el mundo de la privacidad férrea de una encriptación global. Como un ensayo en línea lo explicaba, «desde una primera aproximación, todo propietario de un ordenador menor de treinta y cinco años es ahora un delincuente.» También aumenta la posibilidad de que los intentos de regular la encriptación férrea pudieran, en última instancia, ser combatidos, no entre el Gobierno y los individuales con concepciones no populares, sino entre la RIAA y la gente que descarga la música.

Una propuesta legal alternativa es demandar al proveedor del *software* que comparte archivos por infringimiento contributivo, una propuesta que acabó triunfando, tras largos litigios, en el caso MGM contra Grokster. Pero hacerlo requiere un proveedor que todavía exista, se encuentre bajo la jurisdicción del tribunal y tenga activos de importancia; ninguna de esas condiciones puede garantizarse en casos futuros. Un sistema de iguales descentralizado puede seguir funcionando mucho después de que la organización que lo creó se haya disipado.

Ahí sigue, para algunas formas de propiedad intelectual, la posibilidad de recaudar derechos de autor de clientes de negocios (corporaciones que utilizan Word, cines que proyectan películas). A la larga, incluso esa opción podría reducirse o disiparse. Un mundo en que la privacidad férrea sea lo bastante universal permitiría las empresas virtuales, grupos de individuos unidos por la red, pero dispersos geográficamente y anónimos entre ellos. Incluso si todos ellos usan copias piratas de Word (o el equivalente que haya en ese momento), ningún chivato puede denunciarlos porque nadie, dentro o fuera de la empresa, sabe quiénes son o si han pagado por el *software*.

Marcas de agua digitales

Piensa en el problema en un contexto diferente: imágenes de Internet. Cada imagen se originó en algún sitio y podría pertenecer a alguien.

Pero una vez en línea, cualquiera puede copiarla. No solo es difícil que el propietario del *copyright* evite la copia ilegal, sino que también podría ser difícil incluso que el que copia evite la copia ilegal, ya que podría no saber a quién pertenece la imagen o si se ha puesto a disposición pública.

Una forma de lidiar con estos problemas es la *marca de agua digital*. Usando este *software* especial, el creador de la imagen incrusta en ella información oculta que lo identifica y muestra que está sujeta a *copyright*. En un sistema bien diseñado, la información no tiene un efecto perceptible en cómo ve la imagen el ojo humano y es resistente a que se transforme, lo que significa que todavía está ahí una vez haya convertido un usuario la imagen de un formato a otro, la haya recortado, editado y, quizás, si se creen algunas afirmaciones, incluso impreso y vuelto a escanearla[49].

La marca de agua digital puede usarse de varias formas distintas. La más sencilla es incrustando información en una imagen y haciendo que el *software* que lee la información esté disponible globalmente. Esto reduce el coste de que los usuarios eviten la infracción, haciéndoles fácil que descubran que una imagen se encuentra protegida por *copyright* y quién es el propietario. Ello aumenta el coste de cometer una infracción, al menos en la Web, ya que los motores de búsqueda pueden buscar en Internet imágenes con *copyright* e informar al propietario, que comprueba si el uso gozaba de licencia y, de lo contrario, emprende acciones legales. La existencia de la marca de agua ayudará a probar a ambos a quién pertenece la imagen y que el usuario lo sabía o debería haberlo sabido y, así, es responsable no solo de infracción, sino de infracción deliberada.

La solución obvia es una marca de agua invisible diseñada para ser leída solo por un *software* especial que no se encuentre disponible para el público. No sirve de nada para evitar la infracción involuntaria, pero aumenta sustancialmente los riesgos de la infracción deliberada, ya que el infractor nunca puede estar seguro de que ha eliminado la marca de agua con éxito. Imprimiendo una imagen con una marca de agua tanto visible como invisible, el propietario del *copyright* podría obtener lo

[49] El punto final es importante, ya que proporciona una manera de bloquear el agujero analógico discutido más adelante en el capítulo.

mejor de ambas opciones: proporcionar información para los que no quieren incurrir en un delito y un riesgo de detección para los que sí.

Hay otra manera de que se pueda usar la marca de agua para ejecutar el *copyright*, en un contexto algo distinto. Supón que estamos pensando no en imágenes digitales, sino en programas de ordenador. Supón además que ejecutar la ley de *copyright* contra los vendedores del *software* pirateado no es una opción: se encuentran localizados fuera de la jurisdicción de nuestro sistema jurídico, haciendo negocios de forma anónima, o ambas.

Incluso si los vendedores de las copias pirateadas de nuestro *software* no son anónimos, la gente que los compró originariamente el *software* no lo es. Cuando vendemos el programa, cada copia ha insertado en ella una marca de agua única, un número de serie oculto, a veces denominado huella dactilar digital. Mantenemos un registro de quién se hizo con cada copia y dejamos claro a nuestros clientes que permitir que se copie su copia del programa es una violación de la ley de *copyright* de la cual les hacemos responsables. Si las copias de nuestro *software* aparecen en archivos piratas compramos una, comprobamos la huella dactilar y demandamos al cliente de cuya copia se realizó[50].

La marca de agua digital es un ejemplo de una clase de tecnología que puede usarse para recuperar al menos una parte de lo que se llevaron otras tecnologías. La comodidad de los medios digitales para copiar dificultó la ejecución del *copyright* (a primera vista, difícil hasta el punto de imposible), posibilitando la piratería a nivel individual. Pero la capacidad de las tecnologías digitales para incrustar información invisible y potencialmente indetectable sobre imágenes digitales, combinada con la capacidad de un motor de búsqueda para comprobar mil millones de páginas web en busca de la que contiene una copia sin licencia de una imagen con marca de agua, proporciona la posibilidad de ejecutar la ley del *copyright* contra los piratas individuales. Y la misma tecnología, al incrustar la huella dactilar del adquisidor en el *software* adquirido, proporciona una forma potencial de ejecutar la ley del *copyright* incluso en un mundo de privacidad férrea, no contra

[50] Nótese que esta es una tecnología superior equivalente a una forma de la que se ejecuta actualmente la ley del secreto comercial, con licencia.

piratas anónimos o sus clientes anónimos, sino contra el comprador conocido del que obtuvieron el original para copiarlo.

Mientras que estas son soluciones posibles, no hay garantía de que siempre vayan a funcionar. La marca de agua invisible es vulnerable a alguien lo bastante ingenioso (o con suficiente información de dentro) para dar con el código, descubrir cómo leer la marca de agua y eliminarla. El archivo que representa la imagen o programa se encuentra en manos del pirata. Puede hacer lo que quiera con ella, siempre que sepa lo que hay que hacer.

Es improbable que un individuo que quiera piratear imágenes o *software* tenga la técnica suficiente para dar con cómo eliminar marcas de agua siquiera visibles, ni digamos las invisibles. Para hacerlo, necesita la ayuda de otro que sí la tenga, más fácilmente en forma de *software* diseñado para eliminar marcas de agua visibles e identificar y eliminar las invisibles. Ello plantea la posibilidad de apoyar la solución tecnológica de marcas de agua digitales con prohibiciones legales en la producción y distribución del *software* destinado a vencerla. Esta es la solución empleada por la Ley de Derechos de Autor Digital Millenium (DMCA) de 1998. Prohíbe el *software* cuyo objetivo sea acabar con los esquemas de gestión del *copyright* como la marca de agua digital. Todavía queda por determinar cuánto se puede ejecutar esa prohibición en un mundo de redes y encriptación disponible globalmente.

Cada una de las propuestas para ejecutar el *copyright* que he estado discutiendo tiene limitaciones serias. El uso de huellas dactilares digitales para identificar la fuente de las copias piratas solo funciona si la venta original es lo bastante individualizada como para que el vendedor conozca la identidad del comprador, y aunque podría ser posible vender todo el *software* de esta forma, sería una molestia. Quizás lo más importante sea que esa propuesta funciona muy mal para el *software* que es caro y se emplea globalmente. Una copia legítima de Word podría ser la base de diez millones de copias ilegítimas, con lo que daría lugar a una petición de mil millones de dólares o algo así en daños y perjuicios, y si Microsoft limita sus ventas a los clientes que sean capaces de satisfacer dicha petición y estén dispuestos a arriesgar tanto dinero, no venderá muchas copias de Word. El uso de marcas de

agua digitales para identificar las copias piratas solo funciona si las copias se muestran públicamente, para imágenes digitales en la Web, pero no para una copia pirateada de Word en mi disco duro. Estas limitaciones sugieren que los productores de la propiedad intelectual tienen buenas razones para buscar otras formas de protegerla.

Una forma de solucionar estos problemas sería convertir el ciberespacio, al menos las partes de este que residan en *hardware* bajo la jurisdicción de los tribunales estadounidenses, en una sociedad transparente. Mi ordenador es una localización en el ciberespacio y un objeto físico en el espacio real; en el último formato puede ser regulado por un Gobierno del espacio real, por muy buena que sea mi encriptación. Uno puede imaginarse, en un mundo dirigido por propietarios de *copyright*, un régimen legal que exija que todos los ordenadores estén enlazados y abiertos a motores de búsqueda autorizados a y diseñados para examinar los discos duros en busca de *software*, canciones, películas o imágenes digitales pirateadas.

No pienso que un régimen legal así sea una opción políticamente viable en los Estados Unidos en el futuro cercano, aunque la situación podría ser distinta en otro sitio. Sin embargo, hay versiones privadas que podrían ser más viables, tecnologías que permitan al creador de propiedad intelectual que sea imposible usarla salvo en ordenadores que reúnan ciertas condiciones, una de las cuales podría ser la transparencia frente a los agentes autorizados del propietario.

Para una versión mucho más simple de la misma solución, piensa en estrategias de ejecución del *copyright* posibles si la unidad de procesamiento central de cada ordenador tiene un número de serie de fábrica único para aquel ordenador particular. Una empresa de *software* personaliza cada copia de su producto para que funcione en un solo ordenador, identificado por el número de serie de su unidad central de procesamiento (CPU). El usuario es libre de realizar copias de seguridad y puede dar copias a sus amigos. Pero las copias solo funcionarán en el ordenador para el que se compró el original. A menos, claro, que alguien dé con una forma de o modificar la parte del programa que comprueba el número de serie o modificar otro *software*,

quizás parte del sistema operativo del ordenador, para que mienta al programa sobre cuál es su número de serie[51].

La mayoría de los lectores podrían considerar indignante la idea de ejecutar los términos de una licencia de*software* permitiendo que un ser humano realice una búsqueda aleatoria en su disco duro, pero podría reaccionar de forma muy distinta a la idea de permitir que un programa de su ordenador compruebe su CPU para ver cuál es su número de serie. Algunos podrían estar preocupados por los problemas que surgirán si se hacen con un nuevo ordenador y quieren transferirle su antiguo *software*. Pero es probable que nadie vea un sistema así como una violación intolerable de su privacidad.

Las dos propuestas parecen muy diferentes, pero piensa en algo intermedio. Tu disco duro debe estar abierto a las búsquedas, pero estas solo pueden hacerse por medio de programas informáticos. La única información que los programas son capaces de comunicar a un ser humano es el hecho de que han encontrado *software* sometido a*copyright* en tu disco duro al que no tenías derecho, punto a partir del cual el propietario puede ir a los tribunales para pedir a la autoridad legal que mire tu disco duro.

El asunto planteado por estos ejemplos (hasta qué punto viola tu privacidad ser espiado por una máquina) es uno al que volveremos en un capítulo posterior, en el que consideraremos las implicaciones de usar ordenadores en vez de seres humanos para escuchar las líneas pinchadas.

EL ALAMBRE DE PÚAS DIGITAL

Si usar la tecnología para ejecutar la ley de *copyright* en un mundo donde copiar es fácil no siempre funciona, quizás deberíamos emplear la tecnología para reemplazar la ley de *copyright*. Si usar la ley para mantener lejos a los intrusos y el ganado errante fuera de mis tierras no funciona, quizás debería construir una verja.

---

[51] Recientemente Apple, que ha estado vendiendo canciones en iTunes en un formato protegido, anunció que ahora iba a vender canciones sin protección a un precio ligeramente superior.

Has producido una colección de canciones y deseas venderlas en línea. Para hacerlo, digitalizas las canciones y las insertas en un contenedor protegido criptográficamente —lo que Intertrust, una de las empresas pioneras en la industria, llamó *digibox* (caja digital). El contenedor es un *software* que protege los contenidos del acceso no autorizado mientras que, al mismo tiempo, proporciona y cobra por el acceso autorizado. Una vez estén metidas las canciones en la caja, la distribuyes haciendo que esté disponible para descargar desde tu sitio web.

Descargo el paquete a mi ordenador; cuando lo ejecuto, me aparece un menú con opciones. Si quiero escuchar una canción una vez, puedo hacerlo gratis. A partir de ahí, cada reproducción cuesta cinco céntimos. Si realmente me gusta la canción, por cincuenta céntimos puedo desbloquearla para siempre, con lo que se me permite descargarla tantas veces como quiera. El pago se realiza en línea mediante dinero electrónico, tarjeta de crédito o un acuerdo con un banco colaborador.

La caja digital es un archivo de mi disco duro, así que puedo copiarlo para un amigo. No pasa nada. Si quiere escuchar una de las canciones más de una vez, también tendrá que pagar.

Se te podría haber ocurrido que hay un fallo en el plan de negocios que acabo de describir. El contenedor proporciona una reproducción gratis por cada canción. Para escucharla gratis, todo lo que tiene que hacer el cliente es muchas copias del contenedor y usar una cada vez. Si no, si quiero realizar copias para amigos, puedo pagar cincuenta céntimos una vez para desbloquear el archivo y realizar copias (desbloqueadas) para ellos. Podría ser prudente que la caja digital tenga alguna manera de asegurarse de que el ordenador en que está funcionando es el mismo que en el que se desbloqueó.

Hacer una nueva copia cada vez que reproduces una canción es mucha molestia para ahorrar cinco céntimos. Intertrust no tiene que hacer que su protección sea imposible de salvar, sea de esa forma tan simple o de maneras más complicadas, para que ganen dinero tanto Intertrust como los propietarios de propiedad intelectual. Solo tiene que hacer que vencerla sea más molesto de lo que vale.

Entre el tiempo en que escribí el primer boceto de este capítulo y la revisión final, Intertrust abandonó el negocio al no haber conseguido despegar su propuesta particular de protección tecnológica. La encarnación actual de su propuesta se llama «Digital Rights Management» (Gestión de Derechos Digitales), normalmente abreviada DRM. La idea subyacente es todavía la misma. Los archivos, generalmente de audio o video, se distribuyen en un formato solo accesible con la clave apropiada. La información sobre la clave solo se proporciona a los fabricantes que accedan a construir en su equipo (digamos, un reproductor de CD) restricciones sobre lo que se puede hacer con el archivo. Así, en teoría, el archivo solo puede usarse en equipos diseñados para evitar las copias o restringir su uso de otras formas.

Un problema con esta propuesta es que los archivos se pueden reproducir no solo en equipo construido especialmente para este fin, sino en ordenadores. La empresa que proporciona DRM, por supuesto, se negará a decir a otra gente cómo escribir *software* que desbloquee sus archivos. Pero los archivos mismos están para ser examinados, como lo están los dispositivos autorizados a reproducirlos, lo que dificulta evitar que un programador lo bastante ingenioso revierta la protección para construir una clave apropiada para el *software* sin proporcionar las restricciones sobre el uso que el propietario de la propiedad intelectual desea.

Como en el caso de la marca de agua digital, lo fácil que sea vencer la protección depende mucho de quién lo hace. Es improbable que el cliente individual sea un experto en programación o encriptación, y, por tanto, es improbable que sea capaz de superar incluso las formas simples de protección tecnológica. El riesgo viene de la persona que es experta y coloca su maestría a disposición del público, de forma barata o gratis, en forma de *software* diseñado para romper la protección.

Una propuesta para lidiar con este problema es hacer ilegal crear, distribuir o poseer dicho *software*, estrategia que convirtió en ley la DMCA. Esa ley se enfrenta actualmente a desafíos legales por demandantes que argumentan que publicar información, incluida la información sobre cómo vender el *software* de otra gente, es libertad de expresión, y por tanto está protegida. Incluso si el tribunal rechaza

proteger este tipo particular de expresión, los argumentos de un capítulo anterior sugieren que en el mundo en línea la libertad de expresión podría estar tecnológicamente protegida (por la disponibilidad global de la encriptación y las redes informáticas), con lo que a la larga las partes relevantes de la ley se vuelven inejecutables.

Si la ley no puede proporcionar protección, contra la piratería o las herramientas informatizadas de romper la seguridad diseñadas para vencer la protección tecnológica, la alternativa obvia es tecnológica: cajas fuertes que no puedan forzarse. ¿Es posible?

Para algunas formas de propiedad intelectual (canciones, por ejemplo), no lo es. El problema, a veces denominado «agujero analógico», es que, sea lo fuerte que sea la protección, en algún punto del proceso el cliente consigue reproducir la canción o ver la película, por lo que, después de todo, está pagando. Pero si un cliente está reproduciendo una canción en su propio ordenador en su propia casa, también puede estar reproduciéndola en su propia grabadora, lo que le da una copia de la canción fuera de la caja. Si prefiere un MP3 a un casete, puede reproducir la canción de nuevo en el ordenador, digitalizarla y comprimirla. Para evitar la distorsión por altavoces y micrófono, puede provocar un cortocircuito en el proceso, alimentando las señales eléctricas que normalmente van de los altavoces al ordenador en vez de ser redigitalizados fuera de la caja. Una propuesta similar podría ser secuestrar un libro, video o cualquier otra obra presentada al cliente al completo cada vez que se usa. La protección tecnológica podría convertir el proceso de sacar la obra de la caja digital y ponerla en algún formato utilizable en una molestia, pero una vez lo haya hecho una persona, en un mundo en que la ley del *copyright* es difícil o imposible de ejecutar, la obra está disponible para todos. A falta de hacer registrable el disco duro de cualquiera, la única forma de proteger las obras de este tipo es limitar su consumo a un medio ambiente controlado (mostrar el video en un cine prohibiendo cámaras de video, por ejemplo).

Para otros tipos de ejemplo, la protección segura podría ser una opción más práctica. Piensa, por ejemplo, en una base de datos (imaginaria) compilada por la revista Consumer Reports, diseñada para aconsejar al usuario qué coche comprar. El cuestionario describe el

rango, las preferencias y otra información relevante. La respuesta es un informe personalizado para ese cliente en concreto. Habiendo pagado y recibido el informe, el usuario puede dar una copia a su vecino. Pero es improbable que el vecino lo quiera, ya que no es probable que tenga todos los mismos gustos, circunstancias y constricciones. Lo que el vecino quiere es su propio informe personalizado, que exige otro pago.

Sin el suficiente tiempo, energía y dinero, un pirata podría plantear un millón de preguntas y usar las respuestas para obtener los datos protegidos, pero ¿por qué debería? El pirata puede usar la información robada, puede transmitirla, pero solo tiene una capacidad muy limitada para venderla. Mientras que la protección aumente el coste de reconstruir la base de datos lo suficiente, debería ser razonablemente segura[52]. Para un ejemplo del mundo real de prácticamente esta misma estrategia, piensa en LexisNexis y Westlaw, las bases de datos legales en que confían los abogados y académicos de la ley. No hay nada que evite que descargue un caso legal de Lexis y se lo pase a un compañero que no ha pagado por obtenerlo, pero las posibilidades de que mi compañero esté buscando el mismo caso que yo son bajas.

Para una propuesta diferente para el problema de proteger la propiedad intelectual, piensa en un programa que hace algo muy útil, digamos, el reconocimiento del habla de alta calidad. Lo divido en dos partes. Una, que contiene la mayor parte del código y hace la mayor parte del trabajo, se la doy a el que sea que la quiera. El resto, incluyendo los elementos clave que hacen especial mi programa, reside en mi servidor. Para que funcione la primera parte, tiene que estar intercambiando mensajes continuamente con la segunda parte, por cuyo acceso cobro por minuto.

Una característica elegante de esta solución es que la enfermedad es también la cura. Parte de lo que hace ejecutable el *copyright* es la rápida disponibilidad de las redes informáticas de alta velocidad, lo que permite la veloz distribución del *software* pirateado. Pero las redes informáticas de alta velocidad son precisamente lo que necesitas para la forma de protección que acabo de describir, ya que me permiten hacer

---

52 Una posible propuesta para superar esa forma de protección sería la piratería de fuente abierta, en la que muchos usuarios compartieran la información que obtuvieron individualmente.

que el *software* de mi servidor sea casi tan accesible para ti como el *software* de tu disco duro, y cobrar por ello.

Algunos años después de que escribiera el boceto inicial de esta sección, me di cuenta de que yo mismo era cliente de una propiedad intelectual muy exitosa e innovadora que se encuentra protegida de esta forma. *World of Warcraft*, un juego de rol basado en un sistema en línea de multijugador masivo con algo más de diez millones de clientes, vende el *software* que va en el ordenador del cliente a cualquiera que quiera comprarlo. Pero el *software* del servidor que hace posible que miles de individuos coordinen sus actividades, interaccionen en un mundo común, se encuentra alojado en los propios servidores de Blizzard. Uno puede pensar en *World of Warcraft* y sus competidores como el equivalente de las películas en la tecnología nueva, un equivalente que, a diferencia de las películas, puede protegerse tecnológicamente. Cualquier jugador que quiera puede grabar sus aventuras y enseñarlas a sus amigos. Pero lo que sus amigos quieren es tener sus propias aventuras, y para hacerlo tendrán que pagar la tasa mensual de Blizzard.

Otro ejemplo de la misma propuesta la proporcionan empresas como Pandora y Last.fm. En vez de pedir una canción en concreto, el cliente valora canciones cuando las oye; el servicio usa las valoraciones para decidir qué reproducir después. Piensa en ello como tu propio DJ personalizado.

SUMÁNDOLO TODO

Añadiendo todo lo de este capítulo, tenemos una imagen de la protección de la propiedad intelectual en el mundo de un futuro inmediato con redes de alta velocidad disponibles globalmente, encriptación y copias sencillas. La propiedad intelectual usada públicamente, como las imágenes en la Web, se puede proteger legalmente siempre que no sea lo bastante valiosa para que merezca la pena aguantar la molestia de quitar las marcas de agua ocultas y también siempre que se use en un sitio donde pueda llegar la ley del *copyright*. Esta segunda condición significa que, si nos movemos

hasta un mundo de privacidad férrea, dicha protección desaparece, ya que la ley del *copyright* no sirve de nada si no podemos identificar al infractor. Pero incluso en ese mundo, se puede proteger cierta propiedad intelectual mediante huellas dactilares en cada original y haciendo responsable al comprador de las copias que se hagan de él.

Donde no se puede proteger por ley la propiedad intelectual, todavía podría ser posible protegerla mediante la tecnología. Esa propuesta es de una utilidad limitada para obras que deban revelarse por completo siempre que se acceda a ellas, como una canción. Podría funcionar mejor para obras más complicadas, como una base de datos o un programa de ordenador. Para ambos tipos de obras, la protección será más sencilla si es práctico usar la ley para suprimir el *software* diseñado para vencerla, pero probablemente no lo será.

¿Significa eso que, en el futuro cercano, las canciones dejarán de ser cantadas y se dejará de escribir novelas? No es probable. Lo que sí significa es que aquellos que producen ese tipo de propiedad intelectual habrán encontrado formas de que se le pague que no dependan del control sobre las copias. Para las canciones, una posibilidad obvia es regalar la versión digitalizada y cobrar por los conciertos. Los creadores de películas pueden regalar la película y ganar dinero con los juguetes, que, siendo objetos físicos que se venden en el espacio real, todavía están sujetos a la ley de propiedad intelectual[53]. Otra posibilidad es confiar en la generosidad de los aficionados, en un mundo en que será sencillo enviar por correo una apreciación de diez céntimos al creador de la canción que acabas de disfrutar. Una tercera es regalar la canción junto con un agradecimiento firmado digitalmente a la empresa que te pagó por escribirla y espera que te beneficies de la buena voluntad de los aficionados, el equivalente moderno al viejo sistema del mecenazgo literario.

---

[53] Hasta la fecha, las cinco películas de *Star Wars* han obtenido unos 124 000 millones de dólares en entradas de cine y ventas de productos en todo el mundo, y han entregado una suma divina al distribuidor, Twentieth Century Fox, y a Lucasfilm, la productora. De ese total, 34 000 millones de dólares han provenido de la taquilla mundial y 9000 millones de las ventas de los videojuegos *Battlefront*, los trajes de clon Trooper, figuritas de juguetes de Obi-Wan Kenobi y otros varios aparatos electrónicos, según Lucasfilm (http://money.cnn.com/2005/03/31/news/newsmakers/starwars/index.htm?cnn=yes).

También se encuentran disponibles opciones similares para los autores. El pago normal por derechos de autor de un libro oscila entre el 5% y el 10% de su valor nominal. Muchos lectores podrían estar dispuestos a pagar al autor voluntariamente esa cantidad en un mundo en que la distribución física de los libros no tiene costes. Otros libros se escribirán de la misma forma en que se escriben ahora los artículos de las publicaciones académicas: para difundir las ideas del autor o crear una reputación que pueda usarse para obtener un trabajo, consultar contratos o hablar de oportunidades.

Y PARA NUESTRO PRÓXIMO TRUCO

En el capítulo 4 planteaba la posibilidad de tratar la información transaccional como propiedad privada, con la propiedad asignada mediante acuerdo en el momento de la transacción. Dicha información es una forma de propiedad intelectual y puede protegerse mediante las mismas tecnologías que acabamos de discutir.

Supón, por ejemplo, que estás contento de recibir catálogos en el correo (físico o electrónico), pero no quieres que los extraños sean capaces de recopilar suficiente información sobre ti para permitir el robo de identidad, enfocarte como blanco de extorsión o que usen de alguna otra manera tu información personal contra ti. Alcanzas ambos objetivos haciendo que la información personal generada por tus transacciones (comprar, empleo, alquiler de coche y similares) esté disponible solo en un tipo muy especial de base de datos. La base de datos permite que los usuarios creen listas de direcciones de la gente que sean clientes probables de lo que están vendiendo, pero no les permite obtener datos individualizados de esa gente. Se distribuirá dentro de un contenedor apropiadamente diseñado y protegido criptográficamente o en un servidor protegido, designado para responder cuestionarios pero no para revelar los datos subyacentes. Si los catálogos van a salir por correo electrónico, la base de datos se combina con un servicio de envío. Una copia del catálogo va al servicio, junto con un pago apropiado y mil copias desde ahí hasta mil

direcciones de correo, ninguna de las cuales necesita ser revelada a la compañía de catálogos.

En la versión auténtica de un sistema así, la compañía que dirige la base de datos no sabe tampoco quién eres, ya que la información sale por correo electrónico a través de una cadena de *remailers*; tu dirección de correo electrónico queda sepultada bajo capas de encriptación, con una capa eliminada por cada *remailer*. En una versión más simple, o una diseñada para enviar productos físicos así como mensajes, estás confiando en un intermediario de confianza, una empresa con el negocio de guardar los secretos de sus clientes, una especialidad que solía asociarse a los banqueros suizos.

La información en la base de datos se creó por tus transacciones. En la versión con tecnología más alta, las diriges todas ellas anónimamente, así que nadie salvo tú tiene la información con la que empezar, y puedes controlar quién la tiene posteriormente. En una versión con tecnología más baja, tanto tú como el vendedor comenzáis con la información (lo que compraste y cuándo), pero el vendedor está obligado por contrato a eliminar el registro una vez se complete la transacción. En cualquiera de las versiones, tú preparas que la información esté disponible solo dentro del tipo de base de datos protegida que acabo de describir. Y, si el acceso a esa base de datos es lo bastante valioso, se te paga por ello.

NUEVE

PROGRESO REACCIONARIO: ACADÉMICOS AFICIONADOS Y CÓDIGO ABIERTO

Una lista de la media docena de personas más importantes en la historia reciente de la economía tendría que incluir a David Ricardo; podría incluir también a Thomas Malthus y John Stuart Mill. Una lista similar de geología incluiría a William Smith y James Hutton. En biología seguramente se incluiría a Charles Darwin y Gregor Mendel; en física, a Isaac Newton.

¿Quiénes eran? Malthus y Darwin eran clérigos; Mendel, un monje; Smith, un ingeniero de minas; Hutton vivía de las rentas de sus granjas; Mill, un burócrata y escritor; Ricardo, un prodigio bursátil retirado. De los nombres que he mencionado, solo Newton era profesor de universidad, y para cuando lo fue ya se le habían ocurrido tanto el cálculo como la teoría de la gravitación.

Había figuras intelectuales importantes en los siglos XVII, XVIII y principios del XIX que eran académicos de profesión (Adam Smith, por ejemplo). Pero un gran número, probablemente una mayoría, eran aficionados. En el siglo XX, por otra parte, la mayoría de las figuras importantes de todas las ramas de la erudición han sido académicos profesionales. La mayor parte comenzaron sus carreras profesionales con un curso convencional de educación universitaria, que normalmente les llevó al doctorado.

¿Por qué cambiaron las cosas? Una respuesta posible es el enorme incremento en el conocimiento. Cuando los campos eran nuevos, la mayoría de los académicos no necesitaban acceder a enormes bibliotecas. No había mucha gente en el terreno, la tasa de progreso no era muy rápida, así que las cartas y encuentros ocasionales proporcionaban la comunicación necesaria. A medida que se desarrollaron los campos y se incrementó la especialización, las ventajas de los profesionales (bibliotecas, laboratorios, los compañeros del piso de abajo) se volvieron cada vez más importantes.

Mandar correos electrónicos es tan sencillo como bajar al piso de abajo. La Web, aunque no sea un sustituto completo de una biblioteca, hace que estén disponibles rápidamente cantidades ingentes de información para un número muy grande de personas. En mi campo y muchos otros, se está volviendo común que los autores de artículos académicos pongan sus datos a disposición de la Web de forma que otros académicos puedan comprobar que dicen realmente lo que los artículos afirman que dicen.

Una explicación alternativa para el cambio de aficionado a erudito profesional es la difusión descendente de la educación. En el siglo XVIII, era probable que alguien lo bastante bien educado como para inventar una nueva ciencia fuera un miembro de la clase alta, y, por tanto, tenía altas posibilidades de no necesitar trabajar para ganarse la vida. En el siglo XX, la correlación entre educación y riqueza era mucho más débil.

No es probable que volvamos a la sociedad clasista de la Inglaterra del siglo XVIII. Pero según los estándares de esa sociedad, la mayoría de la gente educada de hoy es rica, lo suficiente para ganarse la vida de forma aceptable y todavía tener tiempo y esfuerzo restantes para dedicarse a sus aficiones. Para una gran parte de la población, y en aumento, la erudición aficionada, como los deportes, música, drama para aficionados, es una opción real. Estos argumentos sugieren que, habiendo cambiado de un mundo de académicos aficionados a un mundo de profesionales, podríamos estar volviendo a cambiar la tendencia. La conjetura se basa en gran parte en mis propias experiencias. Dos ejemplos:

Robin Hanson es actualmente un profesor de economía en la universidad George Mason. Cuando tuve por primera vez contacto visual con él, era un científico de la NASA con una afición curiosa. Su afición era inventar instituciones. Sus ideas (en particular, una propuesta ingeniosa para diseñar mercados para generar información) eran lo suficientemente nuevas y estaban lo bastante bien meditadas para hacer que la correspondencia con él fuera más interesante que con la mayoría de mis compañeros economistas. Eran lo bastante interesantes para otra gente como para que se publicaran. Al final

decidió que su afición era más divertida que su profesión y volvió a clase para sacarse un doctorado en economía.

Una de mis aficiones de los últimos treinta años ha sido cocinar a partir de libros de cocina muy antiguos; mi fuente más temprana es una carta escrita en el siglo VI por un físico bizantino llamado Anthimus a Teodorico, rey de los francos[54]. Cuando comencé, uno tenía prácticamente que reinventar la rueda. No había traducciones impresas de libros de cocina antiguos y muy pocos en las bibliotecas. Casi las únicas fuentes disponibles en inglés, aparte de un pequeño número de libros poco fiables sobre la historia de la cocina, eran unos pocos libros antiguos de cocina ingleses, en particular una colección que había sido publicada por la Early English Text Society en 1888. Conseguí hacerme con una fuente del siglo XVII encontrando una colección de libros poco frecuente que tenía una copia del original y pagando para que la microfilmaran.

La situación ha cambiado dramáticamente durante los últimos treinta años. Los cambios incluyen la publicación de varias fuentes secundarias fiables, fuentes inglesas adicionales y unas pocas traducciones, todo lo cual no podría haber sucedido sin Internet. Pero el mayor cambio es que ahora hay al menos siete traducciones inglesas de libros de cocina antiguos en la Web, disponibles gratuitamente para cualquiera interesado, así como varios libros de cocina inglesa antiguos. La mayoría de las traducciones las hicieron aficionados por diversión. Hay cientos de recetas antiguas sobre las que se ha trabajado (los originales omiten por lo general detalles inesenciales como cantidades, tiempos y temperaturas) en la Web. Hay una lista de correo electrónico que pone en contacto a todos los interesados con un montón de entusiastas experimentados. Alguna de la gente de la lista es cocinera profesional, otros son académicos profesionales. Que yo sepa, ninguno es académico profesional de la historia de la cocina.

Cosas similares están sucediendo en otras áreas. Me dicen que hace mucho que los astrónomos aficionados han representado un papel significativo porque la mano de obra cualificada es una contribución importante a la observación de estrellas. Parece haber una cantidad de interacción cada vez mayor entre los historiadores y grupos que

---

[54] http://www.daviddfriedman.com/Medieval/Medieval.html.

realizan recreaciones históricas aficionadas, a veces espinosa, cuando los aficionados afirman tener unos conocimientos que no tienen, y a veces cordial. Los profesionales, por media, saben mucho más que los aficionados, pero hay muchos más aficionados y algunos de ellos saben bastante. Y el mejor de los aficionados tiene acceso no solo a la información, sino a los demás, así como a cualquier profesional más interesado en la habilidad de la gente con la que se escribe que en sus credenciales.

SOFTWARE DE FUENTE ABIERTA

La erudición aficionada es un ejemplo de la forma en que las rentas crecientes y la tecnología de comunicaciones mejorada hacen más sencillo producir cosas por diversión. Otro es el *software* de fuente abierta.

El ejemplo más famoso es Linux[55], un sistema operativo. La versión original la creó un estudiante de grado finlandés llamado Linus Torvalds. Tras haber hecho él mismo un primer boceto, invitó a todo el resto del mundo a ayudar a mejorarlo. Muchos aceptaron, con el resultado de que Linux es ahora un sistema operativo sofisticado, usado globalmente para una variedad de actividades diferentes. Otro proyecto de fuente abierta, el servidor web Apache, es el *software* mediante el que funcionan una mayoría de páginas de la World Wide Web.

Cuando compras una copia de Microsoft Word, obtienes el código objeto, la versión del programa que ejecuta el ordenador. Con un programa de fuente abierta, obtienes el código fuente, la versión que el programador original escribió, que otros programadores necesitan si quieren modificar el programa y que un humano puede leer. Puedes compilarlo en código objeto para ejecutar el programa, pero también puedes modificarlo y luego compilarlo y ejecutar tu nueva versión del programa.

[55] El núcleo de Linux generalmente se usa con herramientas y bibliotecas del sistema operativo de GNU, así que la combinación a veces se denomina GNU/Linux. http://en.wikipedia.org/wiki/Linux.

La mecánica de la fuente abierta es simple. A alguien se le ocurre una primera versión del *software*. Publica el código fuente. Otra gente interesada en el programa lo modifica —algo que pueden hacer porque tienen el código fuente— y mandan sus modificaciones. Las que acepta el creador van al código base, la versión estándar actual a partir de la que trabajarán otros programadores. En lo más alto del desarrollo de Linux, Torvalds actualizaba el código base diariamente.

Hay muchos programadores, cada uno trabajando en las partes del código que les interesa, así que cuando alguien informa de un problema es probable que haya otro para quien sea obvia su fuente y su solución. «With enough eyeballs, all bugs are shallow[56]» [Con suficientes ojos, todos los *bugs* son superficiales]. Y al ser abierto el código fuente, se pueden encontrar *bugs* y cualquiera interesado puede sugerir mejoras.

Eric Raymond, un portavoz importante del movimiento y autor de un libro sobre él[57], ha apuntado que la fuente abierta tiene sus propias normas y derechos de propiedad. No hay nadie que pueda prohibirte copiar o modificar un programa de fuente abierta. Pero hay propiedad en dos otros sentidos importantes.

Linus Torvalds posee Linux. Eric Raymond posee Fetchmail. Un comité posee Apache. Bajo una licencia de fuente abierta, cualquiera es libre de modificar el código de cualquier forma que quiera, siempre que haga público el código fuente de su versión modificada, manteniendo así la fuente abierta. Pero los programadores quieren que todos trabajen sobre la misma base de forma que cada uno pueda aprovecharse de las mejoras hechas por los demás. Si Torvalds rechaza tus mejoras a Linux, todavía eres libre de usarlas, pero no esperes ayuda. Todo el resto estará trabajando en su versión. Así, la propiedad de un proyecto (la capacidad de decidir lo que entra en el código base) es un derecho de propiedad ejecutado por completo por la acción privada.

Como ha señalado Eric Raymond, dicha propiedad está controlada por normas similares a las normas legales comunes de posesión de tierra. La propiedad de un proyecto va a la persona que lo crea, señorea esa

---

56 "Ley de Linus", atribuida a Linus Torvalds.

57 http://www.catb.org/~esr/; http://www.amazon.com/exec/obidos/tg/browse/-/565706/002–8218385–3353645.

oportunidad programadora particular creando el primer boceto del programa. Si pierde el interés, puede transferir la propiedad a otro. Si abandona el programa, otro puede reclamarlo —comprobar públicamente que nadie está actualmente a cargo de él y luego hacerse cargo públicamente—. El equivalente en la ley de propiedad es la posesión adversa, la norma legal según la cual, si tratas la propiedad como tuya abiertamente durante el bastante tiempo y nadie se queja, es tuya.

Hay una segunda forma de propiedad en fuente abierta: recibir mérito por tu trabajo. Todo proyecto viene acompañado por un archivo que identifica a los autores. Tergiversa ese archivo (sustituye tu nombre, afirmando ser el autor del código que otro escribió) y tu nombre en la comunidad de fuente abierta es Calumnia. Lo mismo pasa en la comunidad académica. Desde el punto de vista de un académico profesional, la violación de *copyright* es un desliz, el robo es problema de otro, el plagio es el pecado definitivo.

Como sugiere este último ejemplo, el movimiento de fuente abierta es simplemente una nueva variación en el sistema bajo la cual se creó la mayor parte de la ciencia moderna. Los programadores crean *software*; los académicos crean ideas. Las ideas, como los programas de fuente abierta, pueden ser usadas por cualquiera. El código fuente, la prueba y los argumentos en los que se basan las ideas, es información pública. Es improbable que un artículo que comienza con «La siguiente teoría es cierta, pero no te diré por qué» convenza a muchos lectores.

Las teorías científicas no tienen propietarios en el sentido en que la tienen los proyectos de fuente abierta, pero en un momento dado en la mayoría de los campos hay un acuerdo considerable sobre lo que es el cuerpo ortodoxo de la teoría. Los académicos pueden elegir ignorar ese consenso, pero si lo hacen, es improbable que se tome su trabajo en serio. El propietario de Apache es un comité. Posiblemente la economía neoclásica pertenece a un comité algo más grande. Un académico puede resistirse a la ortodoxia para comenzar por su cuenta; algunos lo hacen. De forma similar, si no te gusta Linux, eres libre de fundar tu propio proyecto de sistema operativo de fuente abierta basado en tu variación de este. Las ideas heréticas a veces triunfan y los proyectos de

fuente abierta a veces se bifurcan con éxito, pero, en ambos casos, las opciones están en contra.

EL ÉXITO IMPOSIBLE DE JIMMY WALES

Pocos proyectos parecen menos apropiados para la propuesta de fuente abierta que escribir una enciclopedia. Para que sea un éxito, los lectores deben confiar en ella, así que un error en un artículo siembra la duda sobre otros. La estructura es interdependiente; un artículo de un tema frecuentemente necesita referirse a artículos sobre temas relacionados. Claramente la única forma de hacerlo es con una junta editorial central que coordine todo y contrate a expertos de campos variados para escribir los artículos. Por supuesto, he visto argumentos que afirman que la razón del declive de la *Encyclopedia Britannica* desde su punto cumbre en el siglo XX (la undécima edición se considera un clásico) fue el cambio de no pagar sumas sustanciales por artículos, basándose en la teoría de que el prestigio de ser publicado en la *Britannica* era una recompensa suficiente por sí misma. Esto significaba que ofrecían la menor remuneración a los escritores más cualificados, los expertos cuyo prestigio era improbable que creciera por un artículo más de enciclopedia. Si un poco de confianza en los voluntarios, el estatus y pagos no monetarios podían debilitar al líder del mercado, seguramente una confianza total sería fatal para una nueva puesta en marcha.

Resultó no ser así. En 2001, Jimmy Wales creó la Wikipedia como enciclopedia en línea de fuente abierta. No solo se invitó a todo el mundo a realizar contribuciones: todo el mundo tenía la última palabra. Hasta que apareciera alguien más. Cuando Linus Torvalds invitó al mundo a escribir Linux, se quedó con el control del código base; los cambios que no aprobó no se incluyeron. Nadie tiene un poder correspondiente sobre la Wikipedia. Salvo raras excepciones, cualquier artículo puede ser editado en cualquier momento por cualquier persona.

Por increíble que sea, funciona. De vez en cuando hay una sacudida menor cuando un grupo de verdaderos creyentes intenta editar un

artículo para hacer que sostenga su visión del mundo, solo para descubrir que, siempre que hacen un cambio, un malvado de fuera lo deshace. Más frecuentemente de lo que uno podría esperar, un artículo evoluciona hasta un consenso, una afirmación de visiones diferentes con la que ambas partes pueden estar de acuerdo. Funcione como funcione (no he descartado por completo la posibilidad de magia), el resultado seis años más tarde es una obra de referencia masiva que, si bien no es perfecta, es posiblemente tan fiable como las enciclopedias producidas por modelos más convencionales, gratis para todo el mundo y usada por todos; seguramente más global, en línea, que cualquier otro competidor.

EL MERCADO Y LA JERARQUÍA

Una de las extrañas características de un sistema capitalista es lo socialista que es. Las empresas interactúan con clientes y con otras firmas a través de la maquinaria descentralizada del comercio. Pero las firmas mismas son Estados socialistas en miniatura, organizaciones jerárquicas controladas, al menos en teoría, por órdenes de arriba.

Hay una diferencia crucial entre Microsoft y la Rusia de Stalin. Las interacciones de Microsoft con el resto de nosotros son involuntarias. Puede conseguir que la gente trabaje para ella o compre sus productos solo ofreciéndoles un negocio que prefieran a todas las alternativas. No tengo que usar el sistema operativo de Windows a menos que quiera, y, de hecho no lo quiero y no lo hago. Stalin no se enfrentó a dicha constricción.

Una implicación es que, por mala que pueda ser la imagen pública de las grandes corporaciones, existen porque sirven para los propósitos humanos. Los empleados trabajan para ellos porque haciéndolo encuentran una vida mejor que trabajando para ellos mismos; los clientes compran de ellas porque prefieren hacerlo que hacer las cosas por ellos mismos o comprar de otro. Las desventajas asociadas con recibir órdenes, trabajar en los proyectos de otra gente, dependiendo para tu recompensa de la evaluación de tu trabajo realizada por otro,

están contrarrestadas por las ventajas lo suficiente, para mucha gente, para vencerlas[58].

El equilibrio entre las ventajas y desventajas de las grandes organizaciones jerárquicas depende en parte de las tecnologías asociadas con el intercambio de información, la preparación de transacciones, la ejecución de acuerdos y similares. A medida que cambian esas tecnologías, también lo hace ese equilibrio. Cuanto más sencillo es que un grupo disperso de individuos coordine sus actividades, más grande esperamos que sea el papel de la coordinación descentralizada, el mercado más que la jerarquía, en la mezcla total. Esto tiene implicaciones para cómo sea probable que se produzcan los bienes en el futuro: la fuente abierta es un ejemplo sorprendente. También tiene implicaciones para los sistemas políticos, redes sociales y un amplio rango de otras actividades humanas.

Unos años atrás ocurrió un ejemplo en conexión a una de mis aficiones, una dirigida al menos nominalmente por una corporación sin ánimo de lucro controlada por una junta de directores que se autoperpetuaba en el cargo. La junta respondía a los problemas del crecimiento contratando a un director ejecutivo profesional. Actuando aparentemente según su consejo, anunciaron, sin discusión anterior, que habían decidido duplicar las tasas e implementar una propuesta controvertida que se había abandonado previamente en respuesta a una reacción abrumadoramente negativa por parte de los miembros.

Si hubiera sucedido diez años antes, habría habido gruñidos y nada más. Después de todo, la corporación controlaba todos los canales de comunicación oficiales. Cuando su publicación, incluida en el precio de la tasa para miembros, comentó los cambios, los comentarios eran distintivamente desiguales. Los miembros individuales, a los que les dijeron los que estaban al mando que los cambios eran necesarios para la salud de la afición, los habrían aguantado en su mayoría.

Esto no es lo que sucedió. La afición en cuestión había tenido desde hacía mucho un grupo de noticias Usenet en activo asociado a ella. Los miembros incluían a individuales con títulos profesionales, en un amplio rango de áreas relevantes, posiblemente superiores a los de los

[58] Para una discusión mucho más extensa de alguno de estos asuntos, véase Williamson, 1983.

miembros de la junta, el director ejecutivo o los jefes de la corporación. Cada vez que surgía un argumento en defensa de las políticas de la corporación, se daba respuesta, y al menos alguna de esas respuestas era persuasiva. Solo una minoría de los aficionados leían el grupo de noticias, pero era una minoría lo bastante grande como para conseguir que los argumentos relevantes se dispersaran ampliamente. Y el correo electrónico proporcionaba una manera sencilla para que los miembros dispersos que estaban descontentos con los cambios se comunicaran, coordinaran, actuaran. La junta directiva de la corporación se autoperpetuaba (ser miembro no implicaba tener voto), pero estaba formada por voluntarios, gente activa en la afición que estaba haciendo lo que pensaba que era correcto. Descubrieron que muchos de los otros, incluidos aquellos que respetaban, discrepaban y estaban preparados para apoyar su discrepancia con hechos y argumentos. Para cuando la humareda se disipó, cada miembro de la junta directiva que tomó la decisión, salvo aquellos cuyos mandatos habían terminado durante la controversia, habían dimitido; sus relevos revirtieron las decisiones más impopulares. Me resultó un ejemplo interesante de la forma en que la existencia de Internet había invertido el equilibrio entre el centro y la periferia.

Para un ejemplo más comercial, piensa en el anuncio de hace algunos años de que Eli Lilly había decidido subcontratar parte de su investigación química al mundo entero. Lilly creó una subsidiaria, InnoCentive LLC, para mantener una página web con un listado de los problemas químicos que Lilly quería que se solucionaran y los precios, hasta cien mil dólares, que se ofrecían por las soluciones. InnoCentive ha invitado a otras compañías a usar sus servicios para que también se solucionen sus problemas. Para finales de 2001, según una historia en *Wall Street Journal*, han conseguido que «unos mil científicos de India, China y otras partes del mundo» trabajaran en sus problemas[59]. Una serie de otros proyectos que trabajan en líneas similarmente descentralizadas, voluntarios o comerciales, o están en práctica o se han propuesto, incluyendo uno para el desarrollo en fuente abierta de medicamentos para combatir las enfermedades del Tercer Mundo.

---

[59] *Wall Street Journal*, 12/24/01, p. B4. El sitio web es http://www.innocentive.com/.

Un problema que plantea InnoCentive es que la gente que está solucionando los problemas de Lilly podría estar haciéndolo en la nómina de otro. Piensa en un químico contratado para trabajar en un área relacionada con uno de los problemas de la lista. Tiene la tentación obvia de encauzar el trabajo en la dirección del premio de cien mil dólares, incluso si el resultado es ralentizar la consecución de los objetivos del contratante. Es probable que se pille —y despida— a un químico pagado por la firma A mientras que trabaja para la firma B si lo hace en el espacio real. Pero si combina un trabajo del espacio real con un pluriempleo en el ciberespacio (incluso más si parte del trabajo en el espacio real se hacen trabajando a distancia desde su casa), los riesgos podrían ser sustancialmente menores. Así que una posibilidad si la propuesta de InnoCentive sigue adelante es el cambio de pagar por tiempo a pagar por resultados, al menos en algunas categorías de la mano de obra cualificada. En este caso limitativo, el empleo se desvanece y todo el mundo se convierte en un subcontratista, vendiendo rendimiento más que tiempo.

LA GUERRA DE INFORMACIÓN

Hasta ahora hemos estado pensando en formas en que Internet apoya formas descentralizadas de cooperación. También apoya formas descentralizadas de conflicto. Un sistema de comunicación puede usarse como arma, una forma de engañar a otra gente, creando pruebas falsificadas, cumpliendo tus objetivos a expensas de tus oponentes. Piensa en dos ejemplos académicos.

Primer caso: la historia de los cuatro cerditos

Año: 1995. Lugar: Cornell University. Cuatro estudiantes de primer año han recopilado una colección de cartas misóginas tituladas «75 razones por las que las mujeres (zorras) no deberían tener libertad de expresión», y mandaron copias a sus amigos. La colección llega a alguien que la encuentra ofensiva y procede a distribuirla a mucha

gente que comparte esa visión, con lo que produce una avalancha de controversia dentro y fuera de la universidad. La cuestión central es si crear una lista así y usar el correo electrónico para transmitirla es un delito que debería ser castigado o un ejercicio protegido de libertad de expresión.

Al final, Cornell anuncia su decisión. Los estudiantes no han violado ninguna norma de la universidad y, por tanto, no serán sometidos a pena alguna. Sin embargo, han reconocido su error de varias formas:

... además de la carta de disculpa pública que escribieron impresa en el Cornell Daily Sun *el 3 de noviembre de 1995, los estudiantes han ofrecido hacer lo siguiente:*

Cada uno de ellos asistirá al programa «Sex at 7:00» [Sexo a las 7:00] patrocinado por CARE [Defensores de la Educación contra la Violación de Cornell] y la Oficina de Educación Sanitaria en el Gannet Health Center. Este programa trata sobre temas relacionados con la violación en las citas y por parte de conocidos, así como asuntos más generales como relaciones, comunicación y roles de género.

Cada uno de ellos se ha comprometido a realizar 50 horas de servicio comunitario. Si es posible, harán el trabajo en una agencia sin ánimo de lucro cuyo foco primario tenga que ver con el asalto sexual, la crisis de la violación o asuntos similares. Reconociendo que esas agencias podrían ser reacias a aceptar que esos estudiantes trabajen con ellas, los estudiantes realizarán el servicio comunitario en otra parte si la primera opción no está disponible.

Los estudiantes se reunirán con los administradores superiores de Cornell para disculparse en persona y expresar arrepentimiento por sus acciones y la vergüenza y perturbación causadas a la Universidad.

Declaración pública de Barbara L. Krause, Administradora Judicial

Hay al menos dos formas de interpretar ese resultado. Una es que Ms. Krause está diciendo la verdad, toda la verdad y solo la verdad: Cornell no impuso castigo a los estudiantes, ellos mismos se impusieron una pena completamente voluntaria. Parece algo extraño, pero Cornell es una universidad algo inusual.

La interpretación alternativa comienza con la observación de que los administradores de la universidad tienen muchas formas de hacer la vida imposible a los estudiantes. Anunciando públicamente que los estudiantes no habían roto ninguna norma y no estaban sujetos a ningún castigo, mientras que dejan claro de forma privada a los estudiantes que, si planeaban quedarse en Cornell, se les aconsejaba castigarse «voluntariamente», Cornell se metió en un exitoso acto de hipocresía. Públicamente mantuvieron su compromiso a la libertad de expresión mientras que castigaban de forma encubierta a los estudiantes por lo que dijeron.

Alguien que prefería la segunda interpretación pensó en una nueva manera de apoyarla. Se envió un correo electrónico en las vacaciones de Acción de Gracias a los miles de estudiantes, empleados y cuerpo docente de Cornell: 21 132, según sus autores.

CONFIDENCIAL

Me gustaría extender mi más sentido agradecimiento a los numerosos miembros facultativos que me avisaron con respecto al desafortunado incidente de la carta de las «75 razones» que circuló por correo electrónico. Vuestras recomendaciones para tratar con los malhablados «cuatro cerditos» (como pienso en ellos) que circularon esta basura fueron apropiadas y prudentes.

Ahora que hemos tenido tiempo para evaluar la respuesta mediática, pienso que podemos felicitarnos por una estrategia que no solo tuvo éxito en calmar el escándalo, sino que, de hecho, ha aumentado la reputación de la universidad como santuario para aquellos que creen que la «libertad de expresión» es un término relativo que debe comprenderse para implicar límites aceptables de decencia y restricción, con un rápido y severo castigo para aquellos que vayan más allá de esos límites y difundan calumnias sexistas socialmente inaceptables.

Estoy especialmente encantada de informar que los artífices de este asqueroso rollo han sido humillados y silenciados de forma apropiada, sin ninguna indicación externa de que de hecho fuimos nosotros

quienes los disciplinamos. Claramente, ha sido una ventaja para nosotros colocar a los malhechores en una posición en que deban CENSURARSE ELLOS MISMOS, más que dar la impresión de que los estamos censurando nosotros.

…

Atentamente,
Barbara L. Krause, Administradora Judicial

La carta no fue, por supuesto, escrita de verdad por Barbara Krause, como podría haber deducido alguien lo bastante atento como para comprobar la dirección de correo electrónico. Lo escribió y mandó un grupo anónimo que se autodenominaba OFFAL: Luchadores por la Libertad en Línea Liberación Anarquista. La carta era una sátira, efectiva, que daba una imagen creíble y nada atractiva de lo que los autores sospechaban que eran las verdaderas visiones de Ms. Krause. También era un fraude: algunos lectores nunca se habrían dado cuenta de que no era el autor real. En ambas formas, proporcionaba propaganda para la visión de los autores sobre lo que había sucedido en realidad.

Pero hizo más que eso. Los correos no solo se distribuyen fácilmente: se responden fácilmente. Algunos receptores no solo creyeron la carta, estaban de acuerdo con ella y lo dijeron. Puesto que OFFAL había usado no la dirección de correo de Ms. Krause, sino una dirección de correo electrónico que controlaban, esas respuestas llegaron a ellos. OFFAL produjo un segundo correo electrónico que contenía la farsa original, una explicación de lo que hacían y una selección de respuestas.

Resulta que apoyo tus acciones y la resolución de este incidente, pero puesta en las manos erróneas, quizás esta nota podría usarse contra ti.

—

Gracias a dios que mandaste esta nota, algo con un poco de ira y fuego, algo que habla a la emoción y no solo a las legalidades. Espero que tengas razón al afirmar que lo que pasó detrás fue realmente humillante para «ellos».

—-

Estoy de acuerdo con lo que su nota afirma sobre los «cuatro cerditos» (estudiantes que avergonzaron a toda la comunidad de Cornell), pero no creo que yo fuera una de las personas a las que realmente iba destinada tu nota confidencial.... Gran Trabajo en la resolución de un tema de lo más sensible.

—-

Los autores de la lista han recibido una humillación merecida.

Su resumen:

Creemos que el ridículo es un arma más poderosa que las bombas o amenazas de muerte. Y creemos que Internet es el sistema más poderoso jamás inventado para canalizar las protestas populares y la opinión pública a la cara de tiranos mezquinos que buscan imponer sus valores estreñidos en los ciudadanos del día a día que simplemente quieren disfrutar sus libertades protegidas constitucionalmente.

Es difícil no sentir cierta simpatía por los autores. Estaban realizando una argumentación defendible, aunque no estoy seguro de que fuera la correcta, y haciéndolo de una forma ingeniosa y efectiva. Pero al mismo tiempo, como los proveedores de otros tipos de propaganda, estaban combinando un argumento legítimo con uno deshonesto, y fue el último el que dependió de su ingenioso uso de la tecnología de comunicaciones moderna.

El punto correcto fue que las acciones de Cornell se podían interpretar plausiblemente como hipócritas atacando la libertad de expresión mientras fingían apoyarla. El argumento deshonesto fue la implicación de que las respuestas que recibieron proporcionaban apoyo a esa interpretación. Las ocho respuestas que seleccionó OFFAL consistían en seis que apoyaban el correo original, una que la criticaba, una que no hacía ninguna de las dos. Si fuera una selección aleatoria de respuestas, sería una prueba impresionante de su visión de lo que había pasado, pero no tenemos razón para pensar que lo fue. Todo lo que mostraba era que alrededor de media docena de personas de más de veinte mil apoyaba la idea de un castigo encubierto, lo que nos dice muy poco de si eso era lo que estaba sucediendo.

Lo que encuentro interesante del incidente es que demuestra una forma de guerra informativa que se volvió práctica por la naturaleza de la web: costes de transacción muy bajos, anonimato, nada de contacto cara a cara. Considerado una parodia, se podría haber hecho con la antigua tecnología. Como fraude, una manera de engañar a la gente para que revele sus verdaderas creencias fingiendo que se las estaban revelando a alguien que las compartía, podría haberse hecho con la antigua tecnología, pero no de forma tan sencilla. Pero como fraude de producción masiva, una manera de engañar a miles de personas para conseguir que unas pocas revelen sus verdaderas creencias, dependía de la existencia del correo electrónico.

Algunos años atrás, en un grupo de Usenet, leí el siguiente mensaje:

Creo que está bien practicar sexo antes del matrimonio, a diferencia de alguna gente. De esta puedes experimentar distintos tipos de sexo y encontrar al hombre o mujer adecuado que te satisfazca en la cama. Si esperas hasta el matrimonio entonces que pasa si tu pareja no te puede satisfacer, entonces tienes que quedarte con él. Por favor escríbeme y dame tu opinión. También puedes contarme alguna de tus formas de excitar a una mujer porque todavía no he encontrado al hombre apropiado para satisfacerme.

Se me ocurrió que lo que observaba era una variante comercial de la táctica de OFFAL. El mensaje lo leen miles, quizás decenas de miles de hombres. Una centena o así aceptan la oferta implícita y mandan respuestas. Reciben correos electrónicos apropiadamente tentadores como respuesta: los mismos para todos, con solo los nombres cambiados. Continúan la correspondencia. Al final reciben una petición de cincuenta dólares y la amenaza de pasar la correspondencia a la esposa del hombre si no paga el dinero. Los que no están casados lo ignoran; algunos de los casados pagan. La parte responsable ha obtenido mil dólares o así a un coste muy cercano a cero. Chantaje masivo[60].

Uno de mis estudiantes propuso una explicación más simple. El nombre y la dirección de correo asociada al mensaje no pertenecían al

[60] Para una versión antigua, pero ficticia, véase Stout, 1948.

emisor, sino a alguien que no caía bien al emisor. Si tenía razón o no, esa forma de guerra informática se ha usado lo bastante frecuentemente en línea como para haber adquirido su propia denominación: «Joe job». No es una técnica nueva: la versión clásica es un número de teléfono en la pared de un baño de hombres. Pero la red expande enormemente la audiencia.

Una triste historia

La siguiente historia es cierta; los nombres y detalles se han cambiado para proteger a los inocentes.

SiliconTech es una institución de enseñanza superior donde los estudiantes consideran a Cornell, OFFAL y demás como apenas un paso por encima de la Edad de Piedra. Si alguna vez tienen un curso sobre intrusión informática avanzada (que yo sepa, lo tienen), no tendrán problemas para encontrar a estudiantes cualificados.

Alpha, Beta y Gamma eran estudiantes graduados en ST. Los tres provenían de un país del tercer mundo que llamaré Esparta. Alfa y Beta fueron pareja durante casi un año, en un punto llegaron a planear la boda. Terminó cuando Beta dijo a Alfa que ya no quería ser su novia. Durante los meses siguientes Alfa intentó, sin éxito, recuperarla.

Al final, los dos acabaron en un evento social de la Asociación de Estudiantes Espartana; durante el evento, Alfa descubrió que Beta vivía ahora con Gamma. Esto acabó en una acalorada discusión entre los tres; no había testigos externos y los participantes discreparon más tarde sobre lo que dijeron. La versión de Alfa es que amenazó con decir a los otros miembros de la comunidad espartana de ST cosas que dañarían la reputación de Beta y su familia. Esparta era una sociedad sexualmente conservadora y políticamente opresiva, así que es al menos posible que difundir esa información hubiera tenido consecuencias serias. La versión de Beta y Gamma es que Alfa amenazó con comprar una pistola y tener un duelo con Gamma.

Esa misma tarde, después, alguien usó la cuenta de Alfa desde el ordenador en que hizo su investigación para meterse en otra máquina de la universidad y desde ahí falsificar un correo electrónico obsceno a

Beta que fingía venir de Gamma. Durante el proceso, esa misma persona usó la cuenta de Alfa en un superordenador de la universidad. Así como un día más tarde, Beta y Gamma se quejaron del correo falsificado a la organización informática de ST, que lo rastreó hasta la máquina de Alfa, desabilitó su cuenta de sus máquinas y le dejó un mensaje. Alfa, creyendo (según su versión) que Beta y Gamma habían hecho algo para meterle en problemas con la universidad, mandó un mensaje a Gamma diciéndole que tendría que ayudar a Beta con su investigación, ya que Alfa ya no sería responsable de hacerlo.

El día siguiente, se mandó un correo amenazante desde la cuenta de Alfa proveniente de su ordenador de investigación a Gamma. Beta y Gamma llevaron el asunto a las autoridades de ST. Según su versión, Alfa había

1. Acosado a Beta desde que rompieron, haciendo su vida insufrible e impidiendo que realizara su investigación.
2. Mostrado un permiso de armas que tenía y afirmó que iba a comprarse una.
3. Amenazado con matarla.
4. Amenazado con batirse en duelo con Gamma.

Presentaron a las autoridades copias de cuatro correos: los tres descritos, más uno anterior mandado en el momento de la ruptura original. Según Alfa, dos de ellos fueron versiones alteradas de correos que había mandado, dos nunca los había visto.

Dos días después, Beta y Gamma fueron a la policía local con la misma versión más una acusación de que, cuando Alfa y Beta todavía eran pareja, él intentó violarla. Alfa fue arrestado por cargos de acoso y terrorismo, y se fijó una fianza de más de cien mil dólares. Pasó los siguientes cinco meses y medio en la cárcel bajo circunstancias bastante desagradables. El juicio llevó dos semanas; al jurado le llevó tres horas encontrar culpable a Alfa de todos los cargos. Fue soltado. ST procedió a realizar su propio juicio de Alfa por cargos de acoso sexual. Lo encontraron culpable y lo expulsaron.

Cuando me interesé en el caso por primera vez (porque tenía que ver con asuntos de identidad y pruebas de correos electrónicos en una población una década o dos por delante tecnológicamente del resto del mundo), me puse en contacto con el abogado de ST en cuestión. Según

su versión, la situación estaba clara. Las pruebas informáticas demostraban que los mensajes obscenos y amenazadores que se habían originado en última instancia en la cuenta de Alfa, cuya contraseña solo tenía él al haberla cambiado tras su ruptura con Beta. Si bien el jurado podría haberlo absuelto por no tener un arma, Alfa era claramente culpable de delitos contra (al menos) las normas de ST.

Entonces conseguí ponerme en contacto tanto con el abogado de Alfa como con un miembro docente con simpatía hacia Alfa que había estado involucrado en la controversia. De ellos descubrí unos pocos hechos que el abogado de ST había omitido.

1. Todas las cuentas de Alfa usaban la misma contraseña. Antes de su ruptura con Beta, su contraseña había sido «Beta». Después era el nombre de soltera de su madre.

2. Al contrario de los otros estudiantes de grado que habían trabajado con Alfa, y al contrario del testimonio jurado de Beta, los dos habían seguido siendo amigos tras la ruptura y Alfa había seguido ayudando a Beta en su investigación con su propia cuenta informática. Por tanto, es casi seguro que Beta conocía la nueva contraseña. De ahí que ella, o Gamma, o el hermano mayor de Gamma, un gestor profesional de sistemas que resulta que estaba en la ciudad cuando sucedieron los incidentes, podrían haber accedido a las cuentas y realizado todo lo que se acusó a Alfa de hacer.

3. Se suponía que el «intento de violación» había sucedido a principios de la relación. Según el propio testimonio de Beta en el juicio, se fue después de viaje solo con él, durante el cual compartieron una cama. Según otros testigos, normalmente pasaban fines de semana juntos durante algunos meses tras el intento.

4. Durante el juicio hubo pruebas de que muchas de las afirmaciones realizadas por Beta y Gamma eran falsas. En particular, Beta afirmó no haber estado nunca en el despacho de Alfa durante los dos meses después de la ruptura (relevante por el asunto de la contraseña); otros compañeros del despacho testificaron que había estado allí repetidamente. Beta afirmó que se le habían enseñado el permiso de armas de Alfa; la policía testificó que no tenía.

5. Uno de los correos supuestamente falsificados por Alfa se habían creado en un momento en que no solo tenía coartada (estaba en una

reunión con dos docentes), sino que no podía haber anticipado que la fuera a tener, por lo que no podría haberla preparado para programar de alguna forma el ordenador para que hiciera cosas cuando no estuviera presente.

6. La audición de ST la dirigió un miembro docente que había dicho a varias personas que Alfa era culpable y que ST debería librarse de él antes de que hiciera algo de lo que ellos pudieran ser responsables. Bajo la política académica docente, el acusado estaba autorizado a vetar a miembros del comité. Alfa intentó vetar al presidente y se le ignoró. Según mi informador, la audición fue altamente imparcial, con restricciones del comité sobre la introducción de pruebas y argumentos favorables a Alfa.

7. Durante el tiempo que Alfa estuvo en la cárcel esperando el juicio, sus amigos intentaron rebajar su fianza. Beta y Gamma se opusieron enérgica y exitosamente al intento, trataron de presionar a otros miembros de la comunidad espartana de ST para que no testificaran a favor de Alfa, e incluso reunieron un folleto que contenía no solo material de Alfa, sino también historias de fuentes en línea sobre estudiantes espartanos matando amantes o profesores.

Dos versiones diferentes de lo que sucedió de verdad son coherentes con las pruebas. Una, la versión impulsada por Beta y Gamma, convierte a Alfa en la parte culpable y explica la evidencia de que Beta y Gamma estaban mintiendo sobre algunos de los detalles como una combinación de exagerar, errores inocentes y perjurio por parte de testigos amigos de Alfa. La otra, la versión aceptada por al menos algunos de los que apoyan a Alfa, convierte a Beta y Gamma en las partes culpables y a ST como mínimo culpable por negligencia. En esa versión, Beta y Gamma conspiraron para incriminar a Alfa por delitos que no había cometido, seguramente como ataque preventivo contra su amenaza de revelar información cierta pero dañina sobre Beta. Una vez en la cárcel, ¿quién lo iba a creer? Lo consiguieron hasta el punto de encerrarle cinco meses y medio, donde recibió palizas de sus compañeros de prisión, le costó a él y a sus amigos unos veinte mil dólares de gastos legales, y, en última instancia, hicieron que le expulsaran.

Me inclino por la segunda versión, en parte porque creo que está claro que el abogado de ST con el que hablé originariamente intentaba engañarme de forma deliberada ocultando hechos que no solo eran relevantes, sino que contradecían directamente los argumentos que esgrimía. Sospecho de la gente que me miente. Por otra parte, a los abogados, incluso los de instituciones académicas, se les contrata para ayudar al interés de sus clientes, no para revelar la verdad a académicos curiosos, así que incluso si creía que Alfa era culpable, habría preferido ocultar la prueba de que no lo era. Para mis fines presentes, lo que es interesante no es qué parte es culpable, sino el hecho de que cualquiera podría haberlo sido, y los problemas que ese hecho plantea para el mundo en el que vivían y en el que nosotros viviremos.

Lecciones

Las mujeres tienen gustos simples. Pueden disfrutar conversando sobre bebés en brazos y hombres enamorados.

H. L. Mencken, *En defensa de las mujeres*.

La comunicación en línea, en este caso el correo electrónico, lleva normalmente identificación que, a diferencia del rostro, puede falsificarse rápidamente. El caso Cornell demostró una forma en que se podía usar ese hecho: para extraer afirmaciones desprevenidas de alguien haciéndose pasar por alguien en quien tiene razones para confiar. Este caso, según una interpretación, demuestra otra: para herir a alguien persuadiendo a terceras partes de que dijo cosas que en realidad no dijo.

La solución obvia es alguna forma de saber quién mandó qué mensaje. Se supone que los encabezados de un mensaje proporcionan esa información. Como ambos casos demuestran, no lo hacen muy bien. Según la interpretación más simple de los hechos de ST, Alfa usó un procedimiento conocido prácticamente por todos en esa comunidad adelantada para mandar un mensaje a Beta que fingía venir de Gamma. Según la interpretación alternativa, Beta o Gama se hicieron

pasar por Alfa (accediendo a su cuenta con su contraseña) para mandar un mensaje a Beta que fingía venir de Gamma, y así hacer que se culpara a Alfa de hacerlo.

ST proporcionaba un segundo nivel de protección: contraseñas. Las contraseñas las elegía el usuario, de ahí que en muchos casos fueran fáciles de adivinar: los usuarios tienden a elegir contraseñas que puedan recordar. E incluso si hubieran sido difíciles de adivinar, un usuario siempre puede decir a otro su contraseña. Por muy elaborada que sea la seguridad que protege el control de Alfa sobre su propia identificación, hasta el uso de firmas digitales e incluyéndolas, no podía protegerle contra una traición de sí mismo. Alfa estaba enamorado de Beta, y los hombres enamorados son imprudentes.

O quizás podría haberlo hecho. Una solución posible es el uso de *biométrica*, identificación ligada a características físicas como huellas dactilares o patrones de retina. Si ST hubiera estado veinte años por delante de nosotros en vez de solo diez, podrían haber equipado a sus ordenadores con escáneres que comprobaran las huellas dactilares y retinas de los usuarios antes de dejarles iniciar sesión. Es improbable que incluso un hombre enamorado regale sus retinas. Con ese sistema, habríamos sabido qué parte era culpable. Siempre que, por supuesto, ninguno de los estudiantes de SiliconTech, la flor y nata de las mentes jóvenes tecnológicamente precoces, dieran con una forma de engañar a los escáneres biométricos o hackear el *software* que los controla.

Incluso si el sistema funciona, tiene algunas desventajas obvias. Para evitar que alguien edite un correo electrónico real que ha recibido y luego presente la versión editada como si fuera la original (lo que Alfa afirma que hicieron Beta y Gamma), el sistema debe mantener registros de todos los correos que pasan por él. Muchos usuarios podrían objetar por cuestiones de privacidad, aunque hay formas tecnológicas posibles para evitar ese problema[61]. Y las exigencias de la identificación biométrica eliminan no solo la falsificación de identidades, sino también el anonimato, que posiblemente podría tener un efecto relajante sobre la libertad de expresión

---

[61] Uno podría usar un algoritmo unidireccional de *hash* para producir un resumen de cada mensaje y almacenar eso en lugar del mensaje completo. El resumen no puede usarse para reconstruir el mensaje, pero sí para comprobar que no se ha cambiado nada, viendo si todavía funciona con el mismo resumen.

Hasta ahora he dado por hecho implícitamente que se trata de una red informática única con un único propietario, como la de Silicon Tech. Con una red descentralizada como Internet, crear una identidad infalsificable se vuelve un desafío todavía más difícil. Puede hacerse por medio de firmas digitales, pero solo si las víctimas potenciales están dispuestas a tomar las precauciones necesarias para evitar que otra gente obtenga acceso a sus claves privadas. La identificación biométrica, incluso si se vuelve completamente de confianza, todavía es vulnerable al usuario que inserta *hardware* o *software* adicional entre el escáner y el ordenador de su propio sistema y lo usa para mentir al ordenador sobre lo que vio el escáner.

CONTROL DE DELITOS DE FUENTE ABIERTA

Unos años atrás, un estudiante universitario llamado Jason Eric Smith vendió un portátil Mac y algunos accesorios en eBay y lo mandó contra reembolso al comprador, que pagó con un cheque de dos mil novecientos dólares que resultó ser falsificado. Jason, comprensiblemente molesto, «publicó mi historia desgraciada y pidió asistencia en todo tablón de Mac en que podía pensar», y recibió más de cien respuestas ofreciéndole ayuda y apoyo oral, una de las cuales aconsejó un investigador privado en línea que, a partir del número de móvil del comprador, era capaz de conseguir su nombre real y número de teléfono fijo. Los intentos de captar el interés del departamento de policía de Chicago, el FBI y el Servicio Secreto no dieron sus frutos: «te llamaremos más tarde» de los primeros, «no lo bastante grande para interesarnos» de los otros.

Al final, Jason obtuvo una respuesta por correo de otro vendedor que había sido víctima del mismo comprador y sabía de la existencia de otros. Incapaz de conseguir interesar a la ejecución legal, se decidió por una pequeña trampa privada, montó una subasta en eBay del mismo ordenador bajo el nombre de su novia y en tres horas recibió una oferta: del mismo comprador. Los usuarios de Mac de Chicago proporcionaron información adicional sobre el vecindario, que resultó no estar en la ciudad en absoluto sino en los suburbios de Markham. Llamó a la

policía de Markham y esta vez encontró un agente entusiasmado por coger granujas. El agente, vestido con un uniforme de FedEx, realizó el envío y arrestó al criminal con más de diez mil dólares de cheques falsos en su posesión.

La historia obtuvo mucha cobertura en las noticias de entonces, pero me la perdí. La razón por la que la conozco es que, cuando buscaba material para esta parte del capítulo, puse una publicación en mi blog pidiendo ejemplos de control delictivo de fuente abierta. El día siguiente tenía respuestas con enlaces a varias historias, incluida la de Jason. Encontré esta historia de la misma forma que él encontró a su delincuente.

Se puede ver el mismo patrón en una serie de casos más recientes. Uno[62] tenía que ver con coleccionistas de sellos estafados por alguien que compró sellos de baja calidad, «los mejoró» y luego vendió las versiones alteradas por precios superiores. Las víctimas consiguieron convencer a eBay de que se uniera a ellos y cerrara una las cuentas del estafador que pudieran identificarse. Las pérdidas totales fueron, aparentemente, de más de un millón de dólares. Uno de los investigadores privados era un agente del FBI retirado y consiguieron identificar al responsable, pero la última noticia que tengo sobre el caso es que no han conseguido que la ley actúe: por desgracia, este estafador no vive en Markham.

La existencia de Internet facilita la ejecución de la ley de fuente abierta por parte de las víctimas de dos maneras. Hace más fácil que una víctima de un delito obtenga información, y facilita que un economista o historiador aficionado obtenga información. Y hace mucho más sencillo que las víctimas se encuentren las unas a las otras, pongan en común la información y trabajen juntos para encontrar al delincuente. Solo el estadio final del proceso exige la intervención de profesionales pagados para atrapar delincuentes.

O quizás ni siquiera el estadio final. Una noticia reciente describía técnicas organizadas en línea para acosar a los estafadores por correo electrónico usando técnicas un poco como las suyas. Y también podría aplicarse una propuesta descentralizada al problema de identificar y

[62] http://www.msnbc.msn.com/id/17171372/.

filtrar el *spam*, una forma de ejecución completamente legal y completamente fuera del sistema legal.

Todo lo cual plantea la interesante pregunta de si hay oportunidades para el delito de fuente abierta así como para el control delictivo de fuente abierta. Si se me ocurre alguna, me la guardaré para mí.

INTERMEDIO

¿QUÉ ES UNA METAFORA?

Estoy escribiendo estas palabras en un documento metafórico en una ventana metafórica en un escritorio metafórico; el documento está contenido en una carpeta de archivos metafórica representada por una imagen en miniatura de una carpeta de archivos real. Sé que el escritorio es metafórico porque es vertical; si fuera un escritorio real, todo se deslizaría hacia abajo.

Todo esto es familiar para alguien cuyo ordenador emplea una interfaz gráfica de usuario (GUI). Utilizamos esta colección de metáforas en capas por la misma razón que llamamos al acceso no autorizado a un ordenador un asalto, y a un programa de lenguaje mecánico grabado en un chip de ordenador, ilegible para el ojo humano, una escritura. La metáfora nos deja transportar un conjunto de conceptos desde una cosa, la que primero unificó ese conjunto, a otra para la que consideramos que la mayoría del conjunto es apropiado. Las metáforas reducen la dificultad de aprender a pensar sobre cosas nuevas. Las que están bien elegidas lo hacen con un coste en conclusiones erróneas mínimo.

Piensa en la metáfora que subyace en la biología moderna: la evolución como intento. La evolución no es una persona y no tiene un propósito. Tus genes tampoco son gente y tampoco tienen propósitos. Aun así, la lógica de la evolución de Darwin implica que todo organismo tiende a gozar de esas características que poseería si hubiera sido diseñado para el éxito reproductivo. La evolución produce el resultado que obtendríamos si cada gen tuviera un propósito (incrementar su frecuencia en generaciones futuras) y actuara para conseguir ese propósito controlando las características de los cuerpos que construye.

Todo lo afirmado sobre la evolución usando el lenguaje del propósito puede reformularse en términos de variación y selección, el argumento original de Darwin. Pero ya que nos las hemos visto con seres con propósitos durante mucho más tiempo del que nos hemos enfrentado a

la lógica de la evolución darwinista, la versión reformulada está más lejos de nuestras intuiciones; plantear así el análisis lo hace más difícil de entender, más torpe. Por eso los biólogos hablan normalmente en el lenguaje del propósito, como cuando Dawkins tituló su brillante exposición de la biología evolutiva *El gen egoísta*.

Para un ejemplo final, piensa en la programación informática. Cuando escribes tu primer programa, la solución parece obvia: dale al ordenador una serie de instrucciones completa, diciéndole qué hacer. Para cuando has llegadomucho más allá de decirle al ordenador que escriba «Hola, mundo», empiezas a darte cuenta de que un conjunto de instrucciones completa para una serie complicada de alternativas es una red más grande y más compleja de lo que puedas retener en tu mente en un momento.

La gente que diseña lenguajes informáticos se enfrenta a ese problema mediante metáforas. Actualmente las más populares son las metáforas de lenguajes orientados a objetos, como Java y C++. Un programador construye clases de objetos. Ninguno de estos objetos son cosas físicas en el mundo real; cada una existe solo como descripción metafórica de un trozo de código. Aun así, la metáfora (objetos independientes, cada uno con control sobre su propia información interna, interactuando al mandar y recibir mensajes) resulta ser una herramienta extraordinariamente poderosa para escribir y mantener programas, programas más complicados de a lo que ni siquiera un programador con mucho talento podría seguir el rastro si tratara de conceptualizar cada uno como un conjunto interactivo sencillo de comandos.

DELITOS METAFÓRICOS

De vez en cuando leo una noticia sobre un intruso que asalta un ordenador, busca entre los contenidos y se va con alguno de ellos, pero no me lo creo. Mirando a un ordenador sentado en mi mesa, es obvio que la entrada en la CPU no es práctica para algo de un tamaño mucho mayor que un gatito. No hay espacio. Y si uno de mis gatos quiere meterse en mi ordenador, no tiene que romper nada: simplemente

tiene que clavar las garras en el lazo de plástico del lateral (los Mac actuales están diseñados para ser modernizados fácilmente) y tirar.

El «asalto informático» es una metáfora. También lo son las huellas dactilares y las marcas de agua del capítulo 8. Los programadores informáticos tienen dedos y a veces dejan huellas dactilares en los disquetes o CD que contienen su trabajo, pero copiar el programa no copia las huellas.

Las nuevas tecnologías hacen posible cosas que no lo eran, a veces incluso inimaginables, hace cincuenta años. Las metáforas son una forma de encuadrar esas cosas en nuestro patrón de ideas ya existente, representadas en leyes, normas, lenguaje. Ya sabemos cómo pensar sobre la gente que entra en casas de otros y qué hacer al respecto. Estableciendo la analogía entre el acceso no autorizado a un ordenador y entrar en una casa, lo amoldamos a nuestro sistema existente de leyes y normas.

La elección de la metáfora importa. Lo que sucede de verdad cuando alguien «asalta» un ordenador por Internet es que manda mensajes al ordenador, este responde a los mensajes y ocurre algo que el propietario del ordenador no quiere que pase. Quizás el ordenador mande lo que se suponía que era información confidencial. Quizás borre el disco duro. Quizás se vuelva uno de miles de accesorios inconscientes para un ataque de denegación de servicio repartido, mandando miles de peticiones para leer la página web de alguien, con el resultado de que el servidor sobrecargado no pueda procesar todas y la página desaparezca temporalmente de la Web. Quizás vomite *spam* bajo las órdenes de su nuevo maestro.

El ordenador está haciendo lo que desea el *hacker*[63] en vez de lo que desea el propietario. Uno puede imaginarse al *hacker* como un intruso, una persona virtual que viaja por la red, abriéndose camino al interior

---

[63] «*Hacker*» ha llegado a aplicarse a la gente que hace cosas ilegales con los ordenadores, aparentemente como resultado de una falsa etimología; la gente no informática vio el término, adivinó lo que significaba, y adivinaron mal. En la cultura informática, un *hacker* es alguien que hace cosas ingeniosas de formas complicadas y poco convencionales, como un programador que modifica un programa de videojuegos para que funcione el doble de rápido mediante un truco (un *hack*) que podría dejar de funcionar la próxima vez que se actualice el sistema operativo. Me gusta imaginarme a un programador observando a un elefante por primera vez: «¿Cómo coge las cosas? Qué*hack* más brillante». Por eso voy a utilizar «cracker».

del ordenador, leyendo información, borrando información, dando órdenes. Así es como pensamos en ello cuando lo llamamos asalto.

Para ver lo arbitraria que es la elección de la metáfora, piensa en el equivalente de baja tecnología. Quiero entregarte papeles legales. Para hacerlo, mis portadores de la documentación tienen que encontrarte. Llamo a tu número de casa. Si no respondes, digo a los portadores que miren en otro sitio. Si contestas, cuelgo y los mando entrar.

Es probable que nadie llame asalto a lo que acabo de describir. Pero concuerda casi exactamente con la descripción anterior. Tu teléfono es una máquina que has comprado y conectado a la red telefónica para un propósito. Estoy usando tu máquina sin tu permiso para un propósito distinto, uno que podrías desaprobar: descubrir si estás en casa, algo que podrías no querer que supiera. Con solo un pequeño esfuerzo, puedes imaginar a un yo virtual deslizándome por la línea telefónica, asaltando tu teléfono, mirando si estás dentro y volviendo para informar. Una definición temprana del ciberespacio era «donde tiene lugar una conversación telefónica».

Ahora tenemos dos metáforas para el acceso no autorizado a un ordenador: el asalto a una vivienda y una llamada de teléfono no deseada. Tienen implicaciones legales y morales muy distintas.

Piensa en una tercera, a la que los *hackers* se refieren como «ingeniería humana»: engañar a la gente para que les proporcione la información secreta necesaria para acceder a un ordenador. Podría tomar la forma de una llamada de teléfono a una secretaria de un ejecutivo de la empresa fuera de la oficina que necesita acceso inmediato al ordenador de la compañía. La secretaria, cuyo trabajo incluye ayudar a los ejecutivos con sus problemas, responde con las contraseñas que se han pedido. El nombre del ejecutivo podría no ser familiar inmediatamente, pero si fueras la secretaria, ¿querrías exponer tu ignorancia respecto a los nombres de la gente importante de la empresa para la que trabajas?

La ingeniería humana es tanto un medio como una metáfora para el acceso no autorizado. Lo que el *hacker* va a hacer al ordenador es lo que acaba de hacer con la secretaria: llamarlo, fingir ser alguien autorizado a obtener la información que tiene y engañarle para que le provea con esa información. Si comparamos un ordenador no con una casa o un

teléfono, sino con una persona, el acceso no autorizado no es asaltar una casa, sino fraude contra el ordenador.

Ahora tenemos tres maneras muy distintas de encuadrar el mismo acto en nuestras normas, lenguaje e instituciones morales: asalto a una casa, fraude o llamada de teléfono no deseada. La primera es delictiva, la segunda a menudo sancionable mediante responsabilidad civil, la tercera legalmente inocua.

En los primeros casos de delitos informáticos, los tribunales no estaban seguros de cuál era la metáfora apropiada. Más o menos el mismo problema fue el que surgió en los primeros casos de *copyright* informático. Los tribunales no tenían claro si un programa de lenguaje mecánico grabado en la ROM de un ordenador era comparable con una escritura (protegible), *fancy cam* o fotos curiosas (improtegibles, al menos por *copyright*) o (el equivalente más cercano por el que fallaron en el anterior juicio) el rollo de papel que controla una pianola.[64]

En ambos casos, la incertidumbre legal la terminaron las legislaturas: las del Congreso, cuando repasó la ley del*copyright* para incluir explícitamente los programas informáticos; las legislaturas de los estados federales, cuando aprobaron leyes de delitos informáticos que hacían de la intrusión no autorizada un delito. La decisión del *copyright*fue correcta, al menos tal y como se aplicó a la copia literal, por razones que he discutido por extenso en otra parte.[65] El veredicto sobre el caso de la intrusión es menos claro.

Elegir una metáfora

Tenemos tres metáforas diferentes para encuadrar el uso no autorizado de un ordenador en nuestro sistema legal. Una sugiere que debería ser un delito penal; una, responsabilidad civil; una, un acto legal, si bien molesto. Para elegir entre ellas, pensamos en cómo la ley

---

[64] Se encontró improtegible en el caso White-Smith Music Publishing Company contra Apollo Company, 209 U.S. 1 (1908). La metáfora es de John Hersey.

[65] Friedman, 2001, Capítulo 11, en http://www.daviddfriedman.com/LawsOrder draft/laws order ch 11.htm.

tratará los actos en cada caso y por qué podría ser preferible un tratamiento o el otro.

El primer paso es realizar un breve bosquejo de la diferencia entre un delito penal y una responsabilidad civil. Un *delito penal* es algo incorrecto tratado por el sistema legal como un delito contra el Estado. Un caso penal tiene la forma «*El Estado de California contra D. Friedman*». En lo que respecta al Derecho, el Estado de California es la víctima, la persona cuyo ordenador asaltaron es meramente un testigo. Si se va a perseguir judicialmente, cómo hacerlo, si y en qué términos se va a llegar a un acuerdo (un acuerdo fuera del tribunal en un caso penal se llama *plea bargain* [acuerdo entre fiscal y defensa para agilizar los trámites judiciales en un caso penal]) lo deciden los empleados del estado federado de California. El coste del procesamiento judicial lo paga el estado federado y la multa, si hay alguna, se paga al Estado. El castigo no tiene necesariamente conexión con el daño realizado por el acto incorrecto, ya que el delito no es «causar una cierta cantidad de daño», sino «violar la ley».

Una *responsabilidad civil* es un acto incorrecto tratado por el sistema legal como un delito contra la víctima; un caso civil tiene la forma «*A. Smith contra D. Friedman*». La víctima decide si denunciar, contrata y paga el abogado, controla la decisión de si llegar a un acuerdo fuera del tribunal y recibe los daños y perjuicios concedidos por el tribunal. En la mayoría de los casos, el pago de los daños y perjuicios concedido debería equivaler al daño realizado a la víctima por el acto incorrecto: lo suficiente para que la víctima quede en el estado en que estaba antes de la realización del delito.

Una discusión por extenso sobre por qué y si tiene sentido tener ambos tipos de ley y por qué tiene sentido tratar algunos tipos de delitos como responsabilidades civiles y algunos como delitos penales es un asunto para otro libro; los lectores interesados pueden encontrarlo en el capítulo 18 de mi libro *Law's Order*. Para nuestros fines será suficiente observar algunas de las normas legales asociadas con los dos sistemas, algunas de sus ventajas y desventajas y cómo podrían aplicarse a una intrusión informática.

Una diferencia con la que podríamos empezar es que, como norma general, la condena penal exige, a diferencia de la civil, que hubiera

intención de cometer el delito (aunque la definición de intención a veces se lleva muy lejos). Según esto, el acceso no autorizado claramente cumple esa exigencia. O quizás no. Piensa en tres historias, dos de ellas ciertas.

Los límites de la intención

Año 1975. El ordenador es una costosa máquina multiusuario localizada en una instalación dedicada a ello. Un empleado pide una lista de todos los que lo están usando actualmente. Uno de los grupos de iniciales que obtiene pertenece a su supervisor, que está junto a él, obviamente sin usar el ordenador[66].

El ordenador era posesión privada, pero lo usaba la Administración Federal de Energía, así que llamaron al FBI. El FBI logró rastrear el acceso a Bertram Seidlitz, que se había marchado seis meses atrás tras ayudar a montar el sistema de seguridad del ordenador. Cuando registraron su despacho, encontraron cuarenta rollos de papel de impresión que contenían el código fuente de WYLBUR, un programa de edición de textos.

El caso planteó una serie de preguntas sobre cómo la ley existente enmarcaba la nueva tecnología. Grabar secretamente la «conversación» entre Seidlitz y el ordenador, ¿violaba la ley que exigía que las grabaciones de las conversaciones telefónicas se hicieran solo con el consentimiento de una de las partes (o una orden judicial, que no tenían)? ¿Era la otra parte el ordenador; de ser así, accedería? ¿Usar el código de otro para acceder a un ordenador cuenta como obtener propiedad por medio de promesas, representaciones o pretensiones falsas o fraudulentas: el lenguaje de la ley? ¿Se puede cometer fraude contra una máquina? ¿Descargar información comercial secreta, como hacía WYLBUR, era apropiación de propiedad? El tribunal pensó que podría serlo, que se podía, y que lo era: se condenó a Seidlitz.

---

[66] El caso es United States contra Seidlitz, Corte de Apelaciones de Estados Unidos, Cuarto Circuito 589 F.2d 152 (1978); resumido en http://www.daviddfriedman.com/CCP 97/CCP97 outline.html#RTFToC9.

Todavía queda otra pregunta: ¿era culpable? Claramente usó los códigos de acceso de otra persona para descargar e imprimir el código fuente para un programa informático. La cuestión es por qué.

La respuesta de Seidlitz fue muy simple. Creía que el sistema de seguridad del ordenador era seriamente inadecuado. Estaba demostrándolo accediendo al ordenador sin autorización, descargando contenido de dentro e imprimiéndolo. Cuando terminara, planeaba mandar los cuarenta rollos de código fuente a la gente que ahora estaba a cargo del ordenador como demostración de lo débiles que eran las defensas. Se podría sospechar (aunque él no lo dijo) que también planeaba mandarles una propuesta de rehacerles el sistema de seguridad. Si estaba diciendo la verdad, su acceso, aunque no estuviera autorizado, no violaba la ley por la que se le condenó, o cualquier otra ley existente en que pueda pensar.

La prueba más contundente a favor de su historia eran los cuarenta rollos de impresión. Para usar el código fuente, tienes que compilarlo, lo que significa que, primero, tienes que convertirlo en un formato que pueda leer un ordenador. En 1975, el reconocimiento de caracteres óptico, la tecnología mediante la cual el ordenador convierte una imagen de una página impresa en un texto que pueda leer una máquina no existía todavía; incluso hoy en día no es del todo fiable. Si Seidlitz planeaba vender el código fuente a alguien que de verdad lo usara, también estaba planeando en algún punto que alguien escribiera los cuarenta rollos en un ordenador (sin realizar errores, ya que un error podría crear un *bug* en el programa). Podría haber sido mucho más sencillo, en vez de imprimir el código fuente, descargarlo en un casete o disquete. Los disquetes con la capacidad de ser escritos habían aparecido en 1973, con una capacidad de unos 250K; un solo disquete de ocho pulgadas podría almacenar unas cien páginas de texto. Los cuarenta rollos de impresión serían más difíciles de producir y mucho menos útiles que unos pocos disquetes. Por otra parte, la impresión proporcionaría una demostración más impactante de la debilidad de la seguridad del ordenador, especialmente para los ejecutivos que no sabían mucho de ordenadores.

Un problema con usar la ley para los problemas planteados por una tecnología nueva es que el sistema legal podría no estar a la altura del

trabajo. Es lo bastante probable que el juez del caso *EE.UU. contra Seidlitz* nunca hubiera tocado un ordenador, y, aún más probable, que tuviera poca idea sobre lo que era un código fuente o cómo se usaba.

Seidlitz claramente había hecho algo erróneo. Pero decidir si era una broma o un delito exigía algo de conocimiento de la tecnología y las costumbres y cultura circundantes que es improbable que posea un juez cualquiera. En otro caso de acceso no autorizado[67], decidido un año antes, el estado de Virgina había acusado a un estudiante de grado del Instituto Politécnico de Virgina de robar fraudulentamente más de cinco mil dólares. Su delito era acceder a un ordenador al que tenía que acceder para realizar el trabajo por el que estaba ahí: usando las claves y contraseñas de otros estudiantes para acceder a él, porque nadie le había asignado tiempo informático y le daba vergüenza pedirlo. Fue condenado y sentenciado a dos años en la prisión penitenciaria estatal. Se suspendió la sentencia, apeló y en la apelación se le absolvió. El motivo: que había robado servicios, no propiedad. solo la propiedad contaba a efectos de la ley de Virginia, y el valor de las tarjetas informáticas e impresiones era menor que los cien dólares que exigía la ley. Si bien los cargos de hurto mayor seguían sobre él, el Instituto le concedió la titulación universitaria, demostrando lo que pensaban de la seriedad de su delito.

Cuando cuento a mis estudiantes el triste caso de Bertram Seidlitz, me gusta ilustrar la idea con otra historia, con tecnologías de acceso más familiares. Esta vez yo soy el héroe, o quizás el villano.

La escena es la puerta principal de la Facultad de Derecho de la Universidad de Chicago. Estoy ahí porque, durante una visita a Chicago, se me ocurrió que necesitaba comprobar algo en un artículo de la publicación *Journal of Legal Studies* antes de mandar el último boceto de un artículo. La facultad no solo lleva el JLS: lo produce, por lo que seguro que la biblioteca tiene el volumen en cuestión. Mientras compruebo el artículo, quizás puedo pasarme a ver a algunos de mis antiguos compañeros y ver qué tal están.

---

67 Lund contra Virginia, Tribunal Supremo de Virginia 232 S.E.2d 745, 217 Va. 688 (1977), resumido en http://www.daviddfriedman.com/CCP 97/CCP97outline.html#RTFToC8.

Por desgracia, es un domingo de las vacaciones de Navidad; no se ve a nadie dentro y la puerta está cerrada. La solución está en mi bolsillo. Cuando dejé esta facultad el año pasado para asumir mi puesto actual en California, me olvidé de devolver las llaves. Saco mi llavero, encuentro la llave apropiada y abro la puerta principal de la facultad.

En la biblioteca surge otro problema. El volumen que quiero no está en el estante, seguramente porque otro lo está usando. Se me ocurre que uno de los amigos que esperaba ver es un académico de primera en el campo y el editor de JLS. Casi seguro que tiene su propio ejemplar en su despacho, como yo en mi despacho de California.

Llamo a la puerta: no hay respuesta. Está cerrada. Pero en la facultad (un sitio muy amigable), la misma llave abre todos los despachos. La mía está en el bolsillo. Abro la puerta, entro y he ahí el *Journal of Legal Studies* en el estante. Lo cojo, compruebo el artículo y me voy.

Al día siguiente, en el avión de camino a casa, abro mi mochila y descubro que, como de costumbre, puse el piloto automático: en vez de poner el volumen de vuelta en el estante, me lo llevé conmigo. Cuando llego a casa, envío el volumen a mi amigo con una nota de disculpa explicándoselo.

Traduzcamos ahora esta historia en una versión más objetiva y veamos cómo quedo legalmente hablando.

Usando llaves que no tenía derecho legal para poseer, entré en un edificio cerrado al que no tenía derecho legal para entrar, entré en una habitación cerrada a la que no tenía derecho legal para entrar y me fui con un objeto de la propiedad de otro que no tenía autorización para coger. Por fortuna para mí, el valor de un volumen del *Journal of Legal Studies* es considerablemente inferior a cinco mil dólares, así que, aunque posiblemente podría ser culpable de robo según la ley de Illinois, no me afecta la ley federal contra el transporte interestatal de propiedad robada. Aparte del hecho de que el Gobierno Federal no tiene interés especial en la facultad de Derecho de la Universidad de Chicago, los hechos de mi delito fueron casi idénticos a los de Seidlitz. El mío simplemente era una versión de baja tecnología.

Esta historia es casi por completo ficticia, inspirada en el hecho de que realmente me olvidé de devolver las llaves hasta un año o así después de dejar Chicago, así que podría haber entrado en el edificio y en un

despacho si hubiera querido. Pero incluso si así fuera, no habría habido un riesgo serio de nada peor que la vergüenza. Todo el mundoinvolucrado en mi supuesto procesamiento habría entendido los hechos relevantes: que no devolver las llaves es el tipo de cosa que hacen los académicos distraídos, que usar esas llaves de la misma forma en que las has estado utilizando los últimos ocho años, incluso si es técnicamente ilegal, es del todo normal y no exige un intento criminal, que mirar en la copia de una publicación de un compañero sin su permiso cuando no está ahí para dártela es también perfectamente normal, y que la gente distraída a veces sale con cosas en vez de ponerlas donde deberían estar. Seidlitz (dando por hecho que de verdad era inocente) no fue tan afortunado.

Mi tercera historia, como la primera, es cierta[68]. La escena esta vez es un edificio de Oregon que pertenece a Intel. Es el año 1993. El que habla es un empleado de Intel llamado Mark Morrissey.

El jueves 28 de octubre a las 12:30 del mediodía, me di cuenta de que un proceso inusual estaba ejecutándose en un ordenador Sun que administro. Comprobaciones ulteriores me convencieron de que era un programa diseñado para adivinar o *hackear* contraseñas. Fui capaz de determinar que el usuario «merlyn» estaba ejecutando el programa. El nombre de usuario «merlyn» está asignado a Randal Schwartz, un contratista independiente. El programa de *hackear* contraseñas había estado ejecutándose desde el 21 de octubre. Investigué el directorio desde el que se ejecutaba el programa y encontré que el programa era Crack 4.1, un programa potente para descubrir contraseñas. Había muchos archivos situados ahí, incluidos passwd.ssd y passwd.ora. Basado en mi conocimiento del usuario, adiviné que había archivos con contraseñas para la organización Intel SSD y también una compañía externa denominada O'Reilly and Associates. Contacté con Rich Cower de la seguridad de Intel.

La seguridad de Intel llamó a la policía local. Se interrogó exhaustivamente a Randy Schwartz; la policía tenía una grabadora pero

---

68 http://www.lightlink.com/spacenka/fors/ para información general, y http://www.lightlink.com/spacenka/fors/police/intelrep.txt para el informe inicial.

no la usó. Su última versión de lo que dijo fue sorprendentemente detallada, dado que tenía que ver con temas de los que los agentes que interrogaban sabían poco, e impresionantemente diferente de su versión de lo que dijo. Los hechos principales, sin embargo, son razonablemente claros.

Randy Schwartz era un profesional informático muy conocido, autor de dos libros sobre PERL, un lenguaje usado para construir cosas en la Web. Tenía una reputación como el tipo de persona que prefiere disculparse después que pedir permiso de antemano. Una razón por la que Morrissey estaba comprobando el ordenador el jueves por la tarde era asegurarse de que Schwartz no estuviera ejecutando trabajos en él que pudieran interferir con su función. Como dijo en su declaración, «Randal tiene el hábito de usar tanta potencia informática como pueda encontrar».

Schwartz trabajaba para Intel como contratista independiente que ejecutaba partes de su sistema operativo. Accedía al sistema desde su casa usando un portal a través del cortafuegos de Intel que había creado según instrucciones de la empresa para uso de un grupo de fuera de la oficina, pero lo mantuvo para su propio uso. En respuesta a las órdenes de Intel, primero había ampliado su seguridad y después lo había desmantelado. Luego lo recreó discretamente en una máquina diferente y siguió utilizándolo.

Cómo asaltar ordenadores[69]

El sistema informático de Intel, como muchos otros, utilizaba contraseñas para controlar el acceso. Esto plantea un problema obvio de diseño. Para que el ordenador sepa si has introducido la contraseña correcta, necesita una lista de contraseñas frente a las que contrastar la tuya. Pero si hay una lista de contraseñas en alguna parte de la memoria del ordenador, cualquiera que pueda acceder a esa memoria podría ser capaz de encontrar la lista.

---

[69] Para una discusión sobre estas tecnologías de alguien que sabe mucho más que yo al respecto, véase Schneier, 1994, http://www.forum2.org/tal/books/crypto.html.

Puedes solucionar este problema creando una pareja clave pública /clave privada y desechar la clave privada (de forma más general, creando algún procedimiento que encripte pero no desencripte[70]). Siempre que se cree una nueva contraseña, encríptala y añádela a la lista del ordenador de contraseñas encriptadas. Cuando un usuario teclee una contraseña, encríptala y comprueba si lo que obtienes concuerda con una de las contraseñas encriptadas de la lista. Alguien con acceso a la memoria informática puede copiar la lista de contraseñas encriptadas, puede copiar el procedimiento para desencriptarlas, pero no puede copiar un procedimiento para desencriptarlas porque no está ahí. Así que no tiene forma de llegar de la versión encriptada de la contraseña en la memoria del ordenador a la contraseña original que tienen que escribir para obtener el nivel de acceso deseado al (y control sobre el) ordenador.

Un programa como Crack soluciona ese problema adivinando contraseñas, encriptando las suposiciones y comparando el resultado con la lista de contraseñas encriptadas. Si tuviera que adivinar aleatoriamente, el proceso llevaría mucho tiempo. Pero a pesar de las instrucciones de la gente que dirige el sistema, los que crean contraseñas frecuentemente insisten en usar el nombre de su mujer, o su fecha de nacimiento, u otra cosa más sencilla de recordar que V7g9H47ax. No lleva tanto tiempo que un ordenador recorra un diccionario de nombres de pila y cada fecha de los últimos setenta años, encripte cada una y las compruebe de nuevo con la lista. Una de las contraseñas que Randy Schwartz hackeó pertenecía a un vicepresidente de Intel. Era la palabra PRE$IDENT.

La defensa de Randy Schwartz era la misma que la de Bertram Seidlitz. Era responsable de partes del sistema informático de Intel. Sospechaba que su seguridad era inadecuada. La forma obvia de comprobar esa sospecha era ver si podía asaltarla. Romper puertas no es la forma usual de comprobar cerraduras, pero asaltar un ordenador no hace en sí ningún daño.

---

70 Todavía de forma más general, creando alguna forma de encriptación unidireccional o mediante *hash* (una forma de encriptar información que no necesita que tengas la información necesaria para desencriptarla).

Adivinando correctamente una contraseña, usándola para llegar a un archivo de contraseñas encriptadas y usando Crack para adivinar un número considerable de ellas, Randy Schwartz demostró la vulnerabilidad del sistema de Intel. Sospecho, conociendo a los informáticos aunque no a este en concreto, que también se estaba entreteniendo resolviendo el rompecabezas de cómo atravesar las barreras de Intel mientras probaba cuánta inteligencia tenía más que la gente que montó el sistema que estaba hackeando, incluyendo un vicepresidente de Intel particularmente descuidado. Estaba ejecutando Crack de forma simultánea (pero menos exitosa) contra un archivo de contraseñas de un ordenador que pertenecía a O'Reilly and Associates, la compañía que publica sus libros.

Puesto que el sistema informático de Intel contiene mucha propiedad intelectual valiosa protegida (o no) por contraseñas, demostrar su vulnerabilidad podría considerarse un servicio valioso. Intel no lo vio así. Ayudaron activamente al estado de Oregon a procesar a Randy Schwartz por violar la ley de delitos informáticos de Oregon. Acabó sentenciado por dos delitos y mala conducta: acceso no autorizado a, alteración y copia de información de un sistema informático.

Dos hechos me llevan a sospechar que Randy Schwartz podría haber sido la víctima, no el delincuente. La primera es que Intel no proporcionó ninguna prueba de que les hubiera robado ninguna información más que las contraseñas mismas. La otra es que, cuando se detectó que Crack estaba ejecutándose, era «merlyn» quien lo ejecutaba, el nombre de usuario de Randy Schwartz. El programa Crack estaba en un directorio llamado «merlyn». También lo estaban los archivos para el portal a través del que se ejecutaba el programa. Encuentro difícil de creer que un profesional de redes informáticas altamente cualificado intentando robar propiedad intelectual valiosa de una de las empresas mundiales más ricas y de alta tecnología más sofisticada lo hiciera bajo su propio nombre. Si interpreto correctamente las pruebas, lo que en realidad pasó es que Intel usó la ley de delitos informáticos de Oregon para ejecutar sus regulaciones internas contra un subcontratista con el hábito de romperlas. Poner fin al contrato delinfractor es una respuesta más convencional y razonable.

Para ser justos con Intel, debería añadir que casi toda mi información de este caso proviene de un extenso sitio web montado por partidarios de Randy Schwartz (lo bastante extenso para incluir toda la transcripción del juicio)[71]. Ni Intel ni sus partidarios han estado dispuestos a colgar una respuesta. Sin embargo, he intercambiado correos con un conocido que está en posición de saber algo sobre el caso. Mi amigo creía que Schwartz era culpable, pero no estaba dispuesto a ofrecer ninguna prueba.

Quizás era culpable; Intel podría tener razones para mantener su silencio más allá de una mala conciencia. Quizás Seidlitz era culpable. Es difícil, recordando un caso con información muy imperfecta, estar seguros de que mi veredicto sobre su veredicto es correcto. Pero pienso que ambos casos, junto con mi propio robo ficticio, muestran problemas en la aplicación de la ley penal a algo tan ambiguo como el acceso no autorizado a un ordenador, lo que proporciona al menos un argumento limitado para rechazar la metáfora del asalto a favor de una de las alternativas.

¿Es delito copiar? El caso de Bell South

Un problema con tratar de colar el acceso no autorizado en el derecho penal existente es que ese intento podría ser ambiguo. Otro es que no encaja muy bien. El problema viene ilustrado por *EE.UU. contra Neidorf*, narrado de forma entretenida en *La caza de hackers*, la versión de Bruce Sterling de una campaña temprana y chapucera contra el delito informático.

La historia comienza en 1988, cuando Robert Riggs, un estudiante universitario, consiguió acceder a un ordenador que pertenecía a Bell South y descargar un documento sobre el sistema de emergencias del número de emergencias. No encontraba utilidad a la información del documento, que trataba de organización burocrática (quién era responsable de qué para quién), no tecnología. Pero escrito arriba se encontraba «ADVERTENCIA: NO USAR O REVELAR FUERA DE BELLSOUTH O ALGUNA DE SUS SUBSIDIARIAS EXCEPTO BAJO

---

[71] http://www.mids.org/mn/604/remerlyn.html.

CONSENTIMIENTO ESCRITO», lo que hacía que obtenerlo fuera una hazaña y el documento, un trofeo. En consecuencia, mandó una copia a Craig Neidorf, que editaba una revista virtual (distribuida de un ordenador a otro) llamada Phrack. Neidorf cortó la mitad del documento e incluyó lo que quedaba en Phrack.

Al final alguien de Bell South descubrió que su documento secreto estaba circulando informáticamente de forma clandestina y lo ignoró. Algo más tarde, agentes ejecutores de la ley federal envueltos en una caza a gran escala del delito informático descendieron sobre Riggs. A él y Neidorf les acusaron de transporte interestatal de propiedad robada valorada en más de cinco mil dólares: un delito federal. Riggs accedió a declararse culpable: Neidorf se negó y fue a juicio.

Bell South afirmó que producir el documento de doce páginas había costado 79 449 dólares, mucho más de los cinco mil exigidos para ser delito. Al final resultó que habían calculado ese número añadiendo a los costes de producción reales (sobre todo los salarios de los empleados que crearon el documento), el valor completo del ordenador en que se escribió, la impresora en que se imprimió y el *software* del ordenador. Los fiscales federales aceptaron la cifra sin preguntas. Tras las preguntas de la defensa, bajó a simplemente 24 639,05. El caso colapsó cuando la defensa estableció dos hechos: que la advertencia del documento del número de emergencias estaba en cada documento que Bell South producía para uso interno, sin importar lo importante o no importante que fuera, y que la información que contenía se proporcionaba por rutina a cualquiera que la pidiera. Un documento que contenía una versión más por extenso de la información publicada en Phrack, información que Bell South había afirmado que valía poco menos de ochenta mil dólares, se vendió por trece dólares.

En los días antiguos de dormitorios de universidades para un solo sexo había una institución social llamada redada *panty*. Un grupo masculino de estudiantes accedía, sin autorización, a un dormitorio femenino y salía con artículos íntimos de indumentaria. El objetivo no era adquirir ropa interior, sino desafiar a la autoridad de la administración universitaria. Robert Riggs se metió en una redada *panty* virtual y acabó declarándose culpable de un delito. Craig Neidorf recibió el botín de una redada *panty* virtual y lo mostró en su ventana virtual. Por ese acto,

el Gobierno federal intentó condenarle por delitos que podrían haber llevado a una estancia de prisión de más de sesenta años.

Parte del problema, de nuevo, era que la tecnología era nueva, por tanto desconocida para mucha de la gente (policías, abogados, jueces) involucrados en el caso. Viéndoselas con un mundo que no entienden, eran incapaces de distinguir entre una redada *panty* y un robo a un banco.

Otra parte del problema era que la ley bajo la que se procesó el caso se diseñó para lidiar con el robo y transporte de objetos físicos. Era natural plantear las preguntas apropiadas para esa ley, incluyendo cuánto costaba producir el objeto robado. Pero lo que se etiquetó como robo era, en realidad, copiar; después de que Neidorf copiara el documento, Bell Sout todavía lo tenía. La verdadera medida del daño no era lo que costaba producir el documento, sino el coste para Bell Sout de que otra gente tuviera la información. Bell South demostró, por estar dispuesta a vender la misma información a un bajo precio, que consideraba ese coste insignificante. Se procesó a Robert Riggs por una metáfora. Según las pruebas de ese caso, era la metáfora errónea.

¿Penal o civil?

La cifra original de Bell South para el coste de crear el documento del número de seguridad era una que ninguna persona honesta podría haber presentado. Si estás de acuerdo, pregúntate cómo Bell South habría respondido a un empleado que, mandando sus gastos para un viaje de ciento sesenta kilómetros, incluyera el precio completo de su coche: el equivalente preciso de lo que hizo Bell South calculando el coste del documento. El testimonio de Bell sobre la importancia y secretismo de la información contenida en el documento también era falsa, pero no necesariamente deshonesta; el empleado de Bell South que lo dio podría no haber sabido que la firma proporcionaba la misma información a cualquiera que la pidiera. Esas dos afirmaciones falsas representaron un papel principal en un procesamiento penal que podría haber puesto a Craig Neidorf en prisión y que sí le costó a él, a su

familia y los que le apoyaban cientos de miles de dólares en gastos legales.

Mantener a sabiendas falsos testimonios que cuestan a otra gente dinero es normalmente procesable. Pero el testimonio de un testigo en un tribunal tiene privilegios: incluso si es deliberadamente falso, el testigo no es responsable del daño hecho. Puede procesársele por calumnia, pero esa decisión no la toma la parte dañada, sino el Estado.

Supón que hubiera ocurrido el mismo caso bajo la ley civil. Bell South denuncia a Riggs por 79 449 dólares. En el curso del juicio se establece que la cifra estaba inflada de forma descomunal por el demandante, que en cualquier caso este todavía tiene la propiedad, así que tiene una queja solo por el daño realizado por que la información saliera, y que ese daño es cero ya que la información ya estaba disponible públicamente por parte del demandante. No solo Bell South pierde el caso, hay riesgo de que se la denuncie por procesamiento malicioso, que no es confidencial. Además, por supuesto, Bell South, en vez del Gobierno federal, habría pagado los costes de procesamiento. Poner esos casos bajo el derecho de responsabilidad civil habría proporcionado a Bell South un incentivo para comprobar sus hechos y deducir si había sido realmente dañada antes, no después, de que iniciara el caso, ahorrando a todos los involucrados mucho tiempo, dinero y lo desagradable del asunto.

Una ventaja del derecho civil es que el demandante habría podido ser responsable del daño que hizo por afirmaciones que sabía que eran falsas. Otra es que se habría centrado la atención en el asunto relevante: no en el coste de producir el documento, sino en el daño al demandante por la copia. Este asunto es familiar en el contexto de la ley de secretos comerciales, que se acerca mucho más que el derecho penal a concordar los hechos actuales del caso.

Otro problema con penalizar esos actos viene ilustrado por el destino de Robert Riggs. A diferencia de Craig Neidorf, aceptó el acuerdo entre el fiscal y la defensa y podría haber pasado una cantidad sustancial de tiempo en prisión, aunque de hecho se canceló su sentencia después de que el juicio dejara claro que no había hecho nada seriamente grave. Una razón para aceptar declararse culpable, seguramente, era la amenaza de una estancia mucho más larga en prisión si el caso fuera a

juicio y perdiera. El derecho penal, al proporcionar al procesamiento la amenaza de castigos muy severos, plantea el riesgo de que los acusados inocentes pudieran acceder a declararse culpables de un delito menor. Si el caso hubiera sido un procesamiento civil de la víctima, el límite superior efectivo sobre los daños habría sido todo lo que debía Riggs.

Sin embargo, hay otra versión para este argumento. Bajo el derecho civil, el demandante paga el procesamiento. Si es probable que el caso vaya a ser caro y el acusado no tiene el dinero para pagar grandes daños, podría no merecer la pena demandar en primer lugar, en cuyo caso no hay castigo ni incentivo para llevar a cabo la demanda. Ese problema (proporcionar un incentivo adecuado para procesar cuando el procesamiento es privado) lo tocamos en el capítulo cinco y volveremos a él en el doce.

PARTE CUATRO

DELITO Y CONTROL

ONCE

EL FUTURO DEL DELITO INFORMÁTICO

El capítulo anterior discutió el delito informático, pero su tema era la metáfora. Esta vez es el delito.

EL PASADO COMO PRÓLOGO

En los primeros años, los ordenadores eran grandes sistemas autónomos; la mayoría pertenecía a Gobiernos, grandes empresas o universidades. A menudo esas organizaciones los usaban para controlar acciones importantes del mundo real: escribir cheques, registrar las órdenes de pedido, enviar bienes. La táctica obvia para los delincuentes informáticos era obtener acceso a aquellas máquinas y usar la información que contenían: crear órdenes ficticias y usarlas para que se enviaran bienes reales, hacer que se escribieran cheques en pago por servicios no existentes, o, si el ordenador lo usaba un banco, transferir dinero de las cuentas de otra gente a las suyas.

A medida que pasaba el tiempo, se volvió cada vez más común que las grandes máquinas fueran accesibles desde fuera de su localización por líneas telefónicas. Fue una mejora desde el punto de vista del delincuente. En vez de tener que obtener acceso desde una instalación informática (con el riesgo de ser capturado), podía acceder a la máquina desde una distancia, evitando las defensas informáticas y no las puertas cerradas.

Mientras que acceder a los ordenadores para robar dinero o material era la forma más obvia de delito informático, había otras posibilidades. Una era el vandalismo. Un empleado o antiguo empleado descontento podía romper el ordenador de la empresa o borrar sus datos. Pero era un problema menos serio con los ordenadores que con otros tipos de máquinas. Si un vándalo destroza tu camión, tienes que comprar otro. Si rompe tu ordenador, lo único que tienes que hacer es recargar. Incluso si borra tu disco duro, todavía puedes restaurarlo a partir de tu

copia de seguridad más reciente, con lo que solo se pierden los datos más recientes.

Una posibilidad más interesante era la extorsión. En un caso británico, un supervisor de operaciones informáticas para una gran empresa multinacional decidió que era hora de retirarse. Cogió las cintas que eran el almacenamiento masivo del ordenador de la empresa, las cintas de copias de seguridad y el conjunto de copias de seguridad extra que se almacenaban fuera de la instalación, borró la información del ordenador y se fue. Entonces ofreció revender las cintas (que contenían información que la empresa necesitaba para su funcionamiento ordinario) a la firma por solo doscientos setenta y cinco mil libras (unos setecientos mil dólares)[72]

En un mundo con dinero electrónico anónimo, se podría haber realizado el pago y la información se podría haber entregado por la red por medio de un *remailer*. En un mundo de privacidad férrea, podría haber localizado a una empresa delictiva con el negocio de recoger pagos y haber subcontratado la parte recaudadora del proyecto. Por desgracia para el ejecutivo, cometió su delito demasiado pronto. Intentó recopilar el dinero él mismo (en una motocicleta) y le pillaron haciéndolo.

MARAVILLAS DE UN MUNDO CONECTADO

Todavía existen los grandes ordenadores que controlan gran cantidad de material de valor, pero hoy en día por lo general están conectados a redes. Así que hay ciento de millones de pequeños ordenadores, lo que abre algunas posibilidades interesantes.

Unos pocos años atrás, el Club Informático del Caos de Hamburgo, Alemania, demostró una de ellas en la televisión alemana. Lo que habían escrito era un control ActiveX, un fragmento de código descargado de un sitio web al ordenador de un usuario. Se diseñó para trabajar con Quicken, un paquete de contabilidad usado globalmente. Una de las cosas que Quicken puede hacer es pagar facturas en línea. El control que demostraron modificó los archivos de Quicken para añadir

[72] Parker, 1983, pp. 50–51.

un receptor adicional del dinero. Engaña a un millón de personas para que lo descarguen, haz que cada uno te pague diez marcos al mes (una suma lo bastante pequeña para que se den cuenta tras mucho tiempo) y retirarte.

Una de las historias informáticas delictivas clásicas (posiblemente apócrifa) tiene que ver con un programador que informatizó el sistema contable de un banco. Tras unos pocos meses, los trabajadores del banco se dieron cuenta de que algo parecía ir mal: una lenta filtración de dinero. Pero cuando comprobaron las cuentas individuales, todo estaba en equilibrio. Al final, a alguien se le ocurrió el truco. El programador había diseñado el sistema de forma que todos los errores de redondeo fueran a él. Si tenías que recibir 13,436 dólares de intereses, recibías 13,43; su cuenta recibía 0,6 céntimos. Era un fraude modesto: seis décimas partes de un céntimo no es mucho dinero, y normalmente nadie se preocupa de los errores de redondeo. Pero si el banco tiene un millón de cuentas y calcula el interés diariamente, el total asciende a unos cinco mil dólares al día.

Este tipo de fraude se llama «esquema salami»: nadie se da cuenta de que falta un pequeño trozo de un salami. El Club Informático del Caos había inventado una versión de producción masiva. Casi nadie se da cuenta de una filtración de unos pocos dólares de su cuenta al mes, pero, con millones de cuentas, se acumula rápido. Es el viejo delito informático de engañar a un ordenador para que te transfiera dinero modernizado para un mundo con muchos ordenadores conectados, de los cuales cada uno solo controla pequeñas cantidades. Que yo sepa, aún nadie ha puesto en práctica esta forma particular de delito informático, a pesar de la demostración pública de que se puede hacer. Pero alguien lo hará.

Un delincuente moderno que prefiere la extorsión al robo podría hacerse con los contenidos de los ordenadores para pedir rescate usando un control ActiveX descargado o un virus informático y aprovecharse del poder de la encriptación en clave pública. Una vez llega el *software* al ordenador de la víctima, crea un gran número aleatorio y lo usa como clave para desencriptar los contenidos del disco duro, borrando la versión no encriptada mientras lo hace. El paso final

es encriptar la clave usando la clave pública del delincuente y borrar el original.

La próxima vez que se encienda el ordenador, su pantalla muestra un mensaje ofreciendo desencriptar los contenidos del disco duro por veinte dólares en dinero anónimo, mandados al delincuente por medio de un *remailer* apropiado. El dinero debe acompañarse de la clave encriptada, que incluye el mensaje. El extorsionador mandará de vuelta la clave desencriptada y el *software* para desencriptar el disco duro.

Desde el punto de vista del delincuente, el esquema tiene dos características atractivas. La primera es que, ya que el disco duro de cada víctima está encriptado con una clave diferente, no hay forma de que una víctima pueda compartir la información sobre cómo desencriptarla con otra: cada una debe pagar de forma separada. La segunda es que, con muchas víctimas, el delincuente puede establecer una reputación de comerciar honestamente; tras los primeros casos, todos sabrán que, si pagas, se te devuelve de verdad el disco duro. Que yo sepa, nadie lo ha hecho aún, aunque hubo un caso antiguo con una versión menos sofisticada del esquema, usando disquetes en vez de descargas.

¿Qué más se puede hacer en un mundo con muchos ordenadores pequeños conectados? Una respuesta es vandalismo, algo familiar en forma de virus informáticos. Una posibilidad más productiva es imitar a algunos de los primeros delincuentes informáticos y no robar dinero, sino potencia informática. En cualquier instante, millones de ordenadores de escritorio están mordiéndose la uñas mientras sus propietarios comen o piensan sobre qué escribir. Cuando operas millones de instrucciones por segundo, hay un montón de tiempo entre golpes de teclas. El intento más conocido de aprovechar ese poder desperdiciado es SETI, la Búsqueda de Inteligencia Extraterrestre. Es un esfuerzo voluntario mediante el cual un número elevado de individuos permite que sus ordenadores, cuando están desocupados, trabajen en una pequeña parte de un inmenso proyecto de buscar en el pajar de ruido de radio interestelar la aguja de la información que podría decirnos que, en alguna parte de la galaxia hay alguien más. Esfuerzos similares a escala más pequeña se han usado en experimentos para

comprobar lo difícil que es descifrar varias formas de encriptación, otro proyecto que requiere un trabajo a gran escala.

Uno podría imaginar a un ladrón emprendedor robando una parte de ese poder de procesamiento, quizás justificando su delito porque nadie lo estaba usando de todas formas. El enfoque seguiría las líneas de SETI, pero sin su presencia pública. Descarga un *software* adecuado para varios millones de ayudantes en la ignorancia, luego usa Internet para compartir entre ellos la carga de proyectos informáticos muy grandes. Cobra a los clientes por acceder al ordenador más grande del mundo mientras mantienes su naturaleza exacta en secreto comercial. Piensa en Randy Schwartz, que, robara o no secretos comerciales, tenía la reputación de hacerse con todo el poder informático con que podía hacerse. Nadie lo ha hecho. Mi suposición es que nadie lo hará, ya que un acceso continuo es demasiado fácil de detectar. Pero se han implementado repetidamente dos versiones más destructivas.

Una se llama ataque de Denegación de Servicio (DDOS). Para hacerlo, te haces temporalmente con un gran número de ordenadores conectados y les ordenas que pasen todo el tiempo intentando acceder a una página web que pertenezca a una persona u organización que desapruebas. Un servidor web puede mandar copias de su página web a muchos navegadores a la vez, pero no a un número ilimitado. Con las suficientes peticiones llegando lo bastante rápido, el servidor es incapaz de manejar todas y la página desaparece de la Web.

Una segunda razón para hacerse con muchos ordenadores temporalmente que no te pertenecen es solucionar el problema del *spam*, no el problema al que tú y yo nos enfrentamos con bandejas de entrada saturadas por cientos de ofertas de expandir partes variadas de nuestra anatomía, sino el problema al que se enfrenta la gente que manda *spam*. Si lo mandas desde tu propio ordenador, podrías meterte en problemas, si no con los receptores, entonces con tu propio proveedor de servicios de Internet. Una solución es usar un virus informático para modificar muchos ordenadores de otra gente de una forma que te de acceso temporal a ellos y luego usarlos como accesorios inconscientes.

El *spam* mismo proporciona múltiples ejemplos de delitos informáticos posibilitados por la existencia de enormes números de

ordenadores conectados. Nadie con sentido común creería un correo de un extraño de Nigeria ofreciéndole millones de dólares, hasta que primero proporcione alguna pequeña prueba financiera de ser digno de confianza. Pero si le mandas una oferta así a mil millones de direcciones de correo, diez millones de las cuales resultan ser gente real, alcanzarás a la pequeña minoría de esos diez millones que son lo bastante crédulos o avariciosos para caer en el timo. Una pequeña minoría de diez millones de gente puede ser todavía un gran número.

Computación distribuida: la solución de la que surge el problema

La mayoría de los problemas que hemos estado discutiendo tienen que ver con *software* descargado de una página web al ordenador de un usuario. Este *software* se originó como una solución a uno de los problemas de la informática en redes: la sobrecarga del servidor.

Tienes una página web que hace algo para la gente que accede a ella: les dibuja un mapa para enseñarles cómo llegar a una dirección particular, digamos. Dibujar esa imagen (llegar de información de una base de datos a un mapa que pueda leer un ser humano) requiere potencia informática. Incluso si no requiere mucha potencia, cuando mil personas quieren cada una un mapa diferente dibujado al mismo tiempo, esto se suma y el sistema se ralentiza.

Cada una de estas personas está accediendo a tu página desde su propio ordenador. Leer una página web no necesita mucho para informatizar fuentes, así que la mayoría de esos ordenadores están tocándose las narices, operando a una capacidad mucho menor. ¿Por qué no ponerles a todos a trabajar dibujando mapas?

La página web copia en cada uno de los ordenadores un pequeño programa de dibujar mapas: un control ActiveX o un *applet* de Java. Solo tiene que hacerse una vez. A partir de ahí, cuando el ordenador lee la página, esta manda la información necesaria y dibuja el mapa él mismo. En vez de poner todo el trabajo en un ordenador atareado, se divide entre mil ordenadores desocupados. La misma solución (computación distribuida) funciona en juegos multijugador en la red y muchas otras aplicaciones. Es una solución, pero una solución que,

como acabamos de ver, plantea un nuevo problema. Una vez se mete ese programita en tu ordenador, ¿quién sabe qué podría hacer ahí?

Microsoft se enfrenta a este problema usando firmas digitales identificadas por Microsoft para identificar de dónde viene cada control ActiveX. La respuesta de Microsoft a la demostración del Club Informático del Caos de un nuevo uso para un control ActiveX era que realmente no había un problema. Todo cuanto tenía que hacer un usuario para protegerse a sí mismo era decirle a su navegador, mediante una configuración apropiada del nivel de seguridad del Explorer, que no cogiera controles de desconocidos.

Esto da por hecho que nadie puede engañar a Microsoft para que firme códigos falsificados. Puedo pensar en al menos dos formas de hacerlo. Una es conseguir un trabajo en una compañía de *software* respetable e insertar códigos extra en uno de sus controles de ActiveX, que Microsoft firmaría posteriormente. La otra es crear tu propia empresa de*software*, producir *software* útil que use un control ActiveX, añadir una característica adicional sin marcar inspirada en el Club Informático del Caos, hacer que lo firme Microsoft, ponerla en la Web, entonces cerrar el negocio y fugarse a Brasil.

Sun Computer tiene una solución diferente para el mismo problema. Las *applets* de Java, su versión de *software*para la computación distribuida, solo están autorizadas a reproducirse en el *sandbox*, diseñado para tener una capacidad muy limitada para afectar a otras cosas del ordenador, incluyendo archivos almacenados en el disco duro. Un problema con esa solución es que limita las cosas útiles que puede hacer una *applet*. Otro es que incluso Sun se equivoca a veces. La verja alrededor de la *sandbox* podría no estar completamente a prueba de *applets*.

Lo probable es que ActiveX y las *applets* sean historia bien pronto. Sea cual sea la forma de computación distribuida que las suceda, se enfrentará al mismo problema y al mismo conjunto de posibles soluciones. Para ser útil, tiene que ser capaz de hacer cosas en el ordenador del cliente. Cuanto más pueda hacer, mayor es el daño de hacer actividades que el ordenador de ese ordenador desaprobaría. Esto se puede controlar controlando lo que se descarga y teniendo por responsable a la empresa que lo certificó del comportamiento

del *software* o limitando estrictamente lo que se permite que haga cualquier *software* de esta índole: las propuestas de Microsoft y de Sun, respectivamente.

Dolores crecientes

Los lectores con conexión a Internet alta podrían estar preguntándose en este punto si deberían desconectarse. Ni lo creo ni lo he hecho yo mismo.

Hay dos cosas importantes que recordar sobre el tipo de problema que hemos estado discutiendo. La primera es que es tu ordenador, que se encuentra en tu escritorio. Uno de los malos podría ser capaz de hacerse con su control mediante algún truco astuto, haciendo que descargues *software* falsificado o un virus. Pero empiezas con el control, y haga lo que haga el malo, siempre puedes desenchufar la máquina, arrancar a partir de un CD, limpiar el disco duro, restaurar tu copia de seguridad y comenzar de nuevo. La lógica de la situación te favorece. Solo es el diseño del*software* malo y el uso descuidado lo que hace posible que otra gente se haga cargo de tu máquina.

La segunda cosa que hay que recordar es que este es un mundo nuevo y acabamos de llegar. La mayoría de los ordenadores de escritorio están ejecutándose con *software* diseñado originariamente para sistemas autónomos. No es sorprendente que este *software* demuestre frecuentemente ser vulnerable a amenazas que no existían en el ambiente en que se diseñó. A medida que el *software* evolucione en un mundo de redes, muchos de los problemas actuales desaparecerán gradualmente. Hasta la próxima innovación.

El gusano da un giro: clientes engañando a servidores

Hemos estado discutiendo delitos cometidos por un servidor contra clientes: descargarles fragmentos de código que hagan cosas que sus propietarios no aprobarían. Una vez me embarqué en una conversación interesante con alguien que había tenido precisamente el problema

opuesto. Estaba en el negocio de juegos de ordenador, juegos de rol en línea en los que grandes números de personajes, cada uno controlado por un jugador diferente, interactúan en un universo común, aliándose, luchando contra los otros, obteniendo experiencia, volviéndose más poderosos, adquiriendo espadas encantadas, libros de hechizos y similares.

La gente que juega en línea quiere muchos personajes. A medida que se van uniendo más y más personajes, la carga sobre el servidor en que se apoya el juego aumenta, ya que tiene que guardar las características y actividades de un número de personajes cada vez mayor. De forma ideal, un ordenador único debería guardar todo para mantener un universo coherente, pero hay un límite a lo que puede hacer cada ordenador.

Una solución es la computación distribuida. Descargar la mayoría del trabajo al ordenador del jugador. Permite que dibuje las bellas imágenes en la pantalla, mapas de una mazmorra o una visión de un luchador de un monstruo contra el que está luchando. Déjale que almacene cuándo oro tiene el personaje, cuánta experiencia ha acumulado, qué dispositivos mágicos tiene en su posesión, qué armadura en su espalda. El servidor todavía necesita guardar lo fundamental que está compartido (quién está dónde), pero no los detalles. Ahora el juego se equilibra; cuando doblas el número de jugadores, casi doblas la potencia de computación disponible, ya que los ordenadores de las personas nuevas están compartiendo ahora la carga.

Como muchas soluciones, esta viene con un problema. Si mi ordenador está grabando lo fuerte que es mi personaje y los bienes que tiene, esa información se almacena en archivos en mi disco duro. Mi disco duro está bajo mi control. Con un poco de conocimiento especializado sobre cómo se almacena la información (proporcionado, quizás, por un compañero entusiasta en línea), puedo modificar esos archivos. ¿Por qué pasar cientos de horas luchando contra monstruos para convertirme en un héroe con músculos de acero, reflejos como el rayo y una espada mágica, cuando puedo obtener el mismo resultado editando apropiadamente el archivo que describe mi personaje? En el mundo de los juegos en línea, donde muchos jugadores tienen una

técnica sofisticada, son competitivos y no tienen escrúpulos (o, si lo prefieres, donde muchos jugadores consideran las trampas para competir como meramente otra dimensión del juego), aparentemente es un problema real. Le ofrecí una solución; no sé si él, o cualquier otro, ha probado a implementarla.

El servidor no puede molestarse en no perder de vista todos los detalles de todos los personajes, pero probablemente pueda controlar uno de cada cien. Elige un personaje aleatorio y, mientras su ordenador calcula lo que le está sucediendo, ejecuta un cálculo paralelo en el servidor. Síguele unos cuantos días para asegurarte de que sus características siguen siendo lo que deberían. Si lo son, cambia a otro.

¿Y si el personaje ha subido misteriosamente veinte niveles desde la última vez que se conectó? El derecho penal resuelve el problema de evitar delitos que son difíciles de detectar (esparcir basura, por ejemplo) aumentando el castigo para equilibrar la baja probabilidad de imponerlo. Aquí también debería funcionar.

Me conecto al juego donde mi personaje, gracias a cientos de horas jugando con la ayuda de un hackeo cuidadoso de los archivos que lo describen, es ahora un mago de nivel ochenta y tres con una colección espectacular de varitas y anillos mágicos. Hay una sorpresa esperando:

«Te despiertas en el desierto, llevando solo un taparrabos. En tu mano se encuentra un pergamino arrugado.»

«Mira el Pergamino.»

«Parece tu letra, pero inestable y que se convierte en un galimatías al final.»

«Lee el Pergamino.»

En el pergamino se lee:

«No debería haberlo hecho. Meterme en artes prohibidas. Los Demonios se acercan. Me estoy yendo. No, No, No…»

«Mostrar mis estadísticas.»

Nivel: 1.

Posesiones: 1 taparrabos.

El delito no merece la pena.

TERRORISMO DE ALTA TECNOLOGÍA: ¿PESADILLA O PROYECTO DE EMPLEO?

Unos pocos años atrás, participé en una conferencia para aconsejar a un tribunal presidencial que investigaba la amenaza del terrorismo con alta tecnología. Hasta donde pude ver, el tribunal se originó con un ejercicio de la Agencia de Seguridad Nacional (NSA) en que demostraban que, si hubieran sido de los malos, habrían podido hacer un gran daño asaltando ordenadores que controlaban bancos, hospitales y mucho más.

Me fui de la conferencia inseguro de si lo que acababa de ver era una amenaza real o un proyecto de empleo de la NSA, diseñado para asegurarse de que el final de la Guerra Fría no acababa con serios recortes presupuestarios. Sin duda, un grupo de terroristas altamente sofisticados podrían hacer mucho daño asaltando ordenadores. Pero un grupo de terroristas sofisticados también podrían hacer mucho daño con baja tecnología. No he visto pruebas de que el mismo equipo no pudiera haber hecho el mismo daño (o más) sin tan siquiera tocar un ordenador. Unos pocos años después de esa conferencia, un grupo de terroristas no muy sofisticados demostraron cuánto daño podían hacer estrellando aviones contra edificios. Sin necesidad de ordenadores.

Sin embargo, se me ocurrió una contribución positiva a la conferencia. Si realmente crees que terroristas extranjeros asaltando ordenadores para cometer sabotaje masivo es un problema, la solución es proporcionar a la gente que posee ordenadores incentivos adecuados para protegerlos, montar su *software* de forma que sea difícil penetrar. Una forma de hacerlo sería legalizar las intrusiones ordinarias. Si el propietario de un ordenador no puede llamar a la policía cuando encuentra que un adolescente talentoso ha estado metiéndose en sus archivos, tiene un incentivo para hacérselo más difícil al adolescente y protegerse. Cuando los ordenadores de Estados Unidos estén a salvo contra Kevin Mitnick[73], Osama bin Laden no tendrá posibilidad alguna.

---

[73] Posiblemente el más conocido de los primeros delincuentes informáticos; se especializó en usar la ingeniería social para conseguir acceso a los ordenadores, pasó cinco años en la cárcel, y actualmente dirige un negocio de consultoría sobre seguridad informática. http://en.wikipedia.org/wiki/Kevin Mitnick.

DOCE

EJECUCIÓN DE LA LEY X 2

El anterior capítulo trataba del uso de las nuevas tecnologías usadas por delincuentes; este trata de la otra cara de la moneda. Comienzo mirando las formas en que se pueden usar las nuevas tecnologías para ejecutar la ley y algunos riesgos asociados. Entonces continúo (mediante un breve desvío al siglo XVIII) pensando en cómo las tecnologías discutidas en los anteriores capítulos podrían afectar no solo a cómo se ejecuta la ley, sino a quién la ejecuta.

EL CONTROL DEL DELITO CON ALTA TECNOLOGÍA

Los delincuentes no solo son los únicos que pueden usar las nuevas tecnologías; también pueden los policías. En tanto que ejecutar la ley es algo bueno, las nuevas tecnologías que lo hacen más fácil son buenas. Pero la capacidad para ejecutar la ley no es una bendición pura: cuanto más fácil sea ejecutar las leyes, más fácil es ejecutar malas leyes.

Hay dos formas distintas en que nuestras instituciones pueden evitar que los Gobiernos hagan cosas malas. Una es hacer ilegales actos malos particulares. La otra es hacerlos imposibles. Esa distinción apareció en el capítulo 3, cuando defendí que la encriptación no regulada podría servir como la versión del siglo XXI de la Segunda Enmienda: una forma de limitar la capacidad del Gobierno para controlar a sus ciudadanos.

Para un ejemplo menos exótico, piensa en las restricciones a los registros de la Cuarta Enmienda: la exigencia de una orden emitida por una causa razonable. Al menos algunos registros bajo la ley actual (pinchar teléfonos, por ejemplo) se pueden hacer sin que la víctima ni siquiera lo sepa. ¿Cuál es el daño? Si no tienes nada que ocultar, ¿por qué deberías objetar?

Una respuesta es que la capacidad de registrar a cualquiera en cualquier momento, pinchar cualquier teléfono, pone demasiado poder

en las manos de los ejecutores de la ley. Entre otras cosas, les permite recopilar información irrelevante para delitos pero útil para chantajear a la gente para que hagan lo que se les dice. Por razones similares, Estados Unidos, prácticamente sola entre las naciones desarrolladas, nunca ha organizado un sistema nacional de carnet de identidad obligatorio, aunque esto podría haber cambiado para cuando se publique este libro. Un sistema así haría un poco más sencillo ejecutar la ley. También haría más sencillos los abusos por ejecución legal.

La teoría subyacente, que creo que todos comprenden aunque pocos la ponen en palabras, es que un Gobierno con solo un poco de poder puede hacer únicamente las cosas que apruebe la mayoría de la población. Con mucho poder, puede hacer cosas que la mayoría desaprueba, incluyendo, a la larga, convertir una democracia nominal en una dictadura *de facto*. De ahí el delicado equilibrio que pretende proporcionar al Gobierno suficiente poder para evitar la mayoría de los asesinatos y robos, pero no mucho más. ¿Cómo podrían afectar a ese equilibrio las nuevas tecnologías disponibles para la ejecución de la ley?

SABER DEMASIADO

Un agente me para y exige registrar mi coche. Le pregunto por qué. Contesta que mi descripción se acerca mucho a la de un hombre buscado por asesinato. Hace treinta años, podría haber sido un argumento convincente. Pero hoy es menos convincente. La razón no es que los agentes sepan menos, sino que saben más.

Como media, hay unos veinte mil asesinatos anuales en EE.UU. Con veinte mil asesinatos y (supongo) varios miles sospechosos en busca y captura, prácticamente cualquiera encaja con la descripción de al menos uno de ellos. Hace treinta años, los agentes habrían tenido información sobre solo aquellos que están en la cercanía. Hoy pueden acceder a un banco de datos con todos ellos.

Piensa en el mismo problema como podría presentarse en un tribunal. Se comete una violación o asesinato en una gran ciudad. Se dice al jurado que el ADN del acusado concuerda con el del autor del delito, solo hay una posibilidad entre un millón de que concuerde por

casualidad. Obviamente es culpable: esas posibilidades satisfacen fácilmente las exigencias de «más allá de duda razonable».

Hay dos problemas con esa conclusión. La primera es que la afirmación de una entre un millón es falsa. La razón de que sea falsa tiene que ver no con el ADN, sino con la gente. La cifra se calculó bajo el supuesto de que todas las pruebas se hicieron correctamente. Pero hay muchas evidencias de casos pasados de que las posibilidades de que alguien en el proceso, sea el agente que mandó la prueba o el técnico de laboratorio que hizo la prueba, fue o incompetente o deshonesto sean muy superiores a una entre un millón[74].

El segundo problema todavía no es relevante, pero podría serlo pronto. Para verlo, imagina que hemos realizado pruebas de ADN a todo el país para montar una base de datos nacional de información de ADN, quizás como parte de un nuevo sistema nacional de carnés de identidad. Bajo el interrogatorio de la defensa, surge más información. La forma de encontrar al sospechoso de la policía fue buscando en la base de datos de ADN. Su ADN concordaba con la prueba; no tenía coartada, así que lo arrestaron.

Ahora las posibilidades de que sea culpable se reducen drásticamente. La posibilidad de que el ADN de alguien elegido al azar concordara con la muestra tanto como la suya es solo de una entre un millón. Pero la base de datos contiene información sobre setenta millones de hombres en el grupo de edad en cuestión. Por pura casualidad, unos setenta de ellos concordarán. Todo lo que sabemos del acusado es que es uno de esos setenta, no tiene coartada y vive lo bastante cerca de donde sucedió el delito para que sea concebible que lo haya cometido. Fácilmente podría haber tres o cuatro personas que reúnen todas esas condiciones, así que el hecho de que el acusado sea uno de ellos es una prueba muy débil de que sea culpable.

Piensa en el mismo problema en un contexto muy diferente, uno que ha existido desde los últimos veinte años o así. Un economista interesado en delitos tiene la teoría de que la pena de muerte incrementa el riesgo de que se mate a un policía, ya que los acusados de

---

[74] http://www.scientific.org/archive/Houston’s%20Troubled%20DNA%20Crime%20Lab%20Faces%20Scrutiny.htm; http://www.cbsnews.com/stories/2003/03/17/national/main544209.shtml, o véanse múltiples ejemplos en Scheck, Neufeld, and Dwyer, 2000.

asesinato acorralados no tienen nada que perder. Para comprobar su teoría, dirige una regresión, un procedimiento estadístico diseñado para ver cómo factores diferentes afectan al número de policías muertos en servicio. La pena de muerte no es el único factor, así que incluye términos adicionales para variables como la fracción de la población en grupos de edad de alta criminalidad, mezcla racial, nivel de pobreza y similar. Cuando publica sus resultados, informa de que la regresión concuerda con la predicción de la teoría a un nivel de ,05: solo hay una posibilidad entre veinte de que el resultado concuerde tan bien como lo ha hecho por pura casualidad.

Lo que el economista no menciona en el artículo es que la regresión de la que se ha informado es una de las sesenta que dirigió, variando qué factores se incluían, cómo se medían, cómo se suponía que interactuaban. Con sesenta regresiones, el hecho de que al menos una saliera de acuerdo con sus predicciones no nos dice mucho: por pura casualidad, unas tres de ellas deberían.

Cincuenta años más tarde, dirigir una regresión era mucho trabajo, hecho a mano o, si tenías suerte, en una calculadora eléctrica que sumaba, multiplicaba y no mucho más. Hacer sesenta de ellas no era una opción práctica, así que el hecho de que la regresión de alguien concordara con su teoría en un nivel de ,05 era una prueba de que la teoría era correcta. Hoy en día, cualquier académico (prácticamente cualquier niño de colegio) tiene acceso a un ordenador que puede realizar sesenta regresiones en unos pocos minutos. Esto hace sencillo hacer una búsqueda de especificación, intentar muchas regresiones diferentes, cada una especificando la relación de forma un poco distinta, hasta que encuentres una que funcione. Incluso puedes encontrar paquetes estadísticos que lo hacen por ti.

Así que el hecho de que tu artículo informe de una regresión exitosa ya no proporciona mucho apoyo a tu teoría. Como mínimo, tienes que informar de las distintas especificaciones que probaste, dar un resumen verbal de cómo salió y resultados detallados para unas pocas de ellas. Si reamente quieres persuadir a la gente tienes que hacer que tus datos estén completamente disponibles, idealmente por Internet, y dejar que otra gente dirija tantas regresiones sobre el tema de formas tan distintas como quieran hasta que se convenzan ellos mismos de que la

relación que encontraste realmente está ahí, no es una ilusión creada por una selección cuidadosa de los resultados de los que informaste.

Todos esos ejemplos (la parada policial sobre la sospecha, la prueba de ADN, la búsqueda de especificación) tienen que ver con el mismo asunto. Incrementar el acceso a la información hace más fácil encontrar pruebas para la respuesta correcta. Pero también hace más sencillo encontrar pruebas para la respuesta errónea.

Si eres el que busca pruebas, la información adicional es un activo. El investigador puede presentar la búsqueda especificativa y usar sus resultados para mejorar la teoría. El policía de tráfico puede comprobar la base de datos de sospechosos buscados, ver que se informó de que se vio por última vez a la persona con cuya descripción concordé en la otra parte del país, y decidir no molestarse en pararme. El policía, habiendo localizado varios sospechosos que concuerdan con la prueba de ADN, puede meterse en un intento serio de ver si uno de ellos es culpable y solo realizar un arresto si hay suficientes pruebas adicionales para condenar. Desarrolla la tecnología un poco más y la policía, incapaz de encontrar una concordancia para el ADN del sospechoso de su base de datos, puede, en lugar de ello, buscar a sus parientes, y, habiendo encontrado candidatos plausibles, continuar a partir de ahí su investigación.

Pero en cada caso la información adicional también hace más sencillo generar pruebas falsas. El policía de tráfico que realmente quiera pararme por mi color de piel o mi matrícula de otro estado federal, o con la esperanza de encontrar algo ilegal y que se le ofrezca un soborno para no informar, puede afirmar honestamente que concuerdo con la descripción de un hombre en busca y captura. El fiscal del distrito que quiere una buena tasa de condena antes de su próxima campaña para obtener un puesto alto puede presentar la concordancia de ADN y omitir cualquier explicación de cómo se obtuvo y lo que realmente significa. Y el investigador académico, desesperado por publicaciones para reafirmar su petición de tenencia, puede recordar selectivamente solo esas regresiones que salieron bien. Si queremos evitar un comportamiento así, debemos cambiar nuestras normas y costumbres en consecuencia, aumentando el estándar de cuántas pruebas se

requieren para reflejar cuánto más fácil se ha vuelto fabricar pruebas, incluso para cosas que no son verdad.

TODO TELÉFONO

El héroe de *El analista del presidente* (James Coburn), tras haber pasado gran parte de la película escapando de varios tipos malos que quieren secuestrarlo y usarlo para influenciar a su paciente estrella, ha escapado temporalmente de sus perseguidores y ha llegado a una cabina. Llama a un amigable agente de la CIA (Godfrey Cambridge) para que venga a rescatarlo. Cuando intenta abrir la cabina, la puerta no se abre. Por la carretera viene un camión de una compañía telefónica cargado de cabinas. La grúa del camión recoge la cabina del analista, la deposita en la parte trasera, la reemplaza por una cabina vacía y arranca. Un minuto más tarde desciende un helicóptero con el agente de la CIA y un agente de la KGB que es su aliado temporal. Miran incrédulos a la cabina telefónica vacía. El estadounidense habla primero:

«No puede ser. ¿Todos los teléfonos de Estados Unidos están pinchados?»

La respuesta (tendrás que imaginarte el acento)

«¿Dónde crrees que estás, en Rusia?»

Una gran escena de una película muy divertida. Pero podría no ser una broma mucho más tiempo.

Avancemos hasta el debate sobre la propuesta de ley de escuchas digitales, la legislación impulsada por el FBI para exigir que las compañías telefónicas proporcionen instalaciones a los agentes ejecutores de la ley para pinchar líneas telefónicas digitales. Una cuestión que plantearon los críticos a la legislación fue que el FBI parecía estar exigiendo la capacidad para pinchar simultáneamente un teléfono de cada cien. Mientras que esa cifra era probablemente una exageración (no había un acuerdo sobre el significado exacto de la capacidad que pedía el FBI), no era demasiada exageración.

Como afirmó el FBI, esto no significa que fueran a usar toda esa capacidad. Para ser capaces de pinchar un 1% de los teléfonos de un sitio en particular (digamos, un sitio con muchos traficantes de drogas), necesitaban la capacidad para pinchar un 1% de los teléfonos de todas partes. Y la cifra del 1% solo se aplicaría en partes del país donde el FBI pensara que podría necesitar una capacidad así e incluía no solo escuchas, sino también formas de vigilancia menos intrusivas, como registrar quién llamó a quién, pero no lo que dijeron.

Cuando realizaron la petición, la tasa de escuchas era de menos de mil al año, no todas al mismo tiempo. Incluso tras conceder al FBI el beneficio de toda duda posible, la capacidad que pedían solo era necesaria si estaban contemplando un enorme incremento de la vigilancia telefónica.

El FBI defendió la legislación por ser necesaria para mantener el *statu quo*, para impedir que los desarrollos en la tecnología de las comunicaciones redujera la capacidad de la ejecución legal para llevar a cabo interceptaciones bajo orden de un tribunal. Los críticos argumentan que no había pruebas de que existiera tal problema. Mi propia sospecha es que la propuesta estaba motivada por la tecnología, sin duda, pero no por esa tecnología.

El primer paso es preguntar por qué, si pinchar teléfonos es tan útil como afirman los portavoces de los ejecutores de la ley, hay tan pocas de ellas y producen tan pocas condenas. La cifra de 1995 fue un total de 1058 interceptaciones autorizadas a todos los niveles: federal, estatal y local. Fueron las responsables de un total de 494 condenas, la mayoría por delitos de drogas. Las condenas totales por droga de ese año, solo a nivel federal, fueron más de dieciséis mil.

La respuesta no es desgana de los tribunales para autorizar escuchas telefónicas. La Agencia de Seguridad Nacional, después de todo, hace que autorice sus consultas un tribunal especial, del que se dice en todas partes que nunca ha rechazado una petición. La respuesta es que las escuchas son muy caras. Algunas estimaciones aproximadas de Robin Hanson[75] sugieren que, de media, en 1993 costaron más de cincuenta

[75] Hanson, 1994; también disponible en la Web en http://www.hss.caltech.edu/~hanson/wiretap-cacm.html.

mil dólares cada una. La mayor parte del coste era el de mano de obra, el tiempo de agentes escuchando 1,7 millones de conversaciones a un coste de treinta y dos dólares por conversación.

Ese problema se ha solucionado. El *software* para transformar el habla en texto ahora está disponible globalmente en el mercado. Usando ese *software*, puedes hacer que un ordenador escuche, transforme el habla en texto, busque en el texto palabras clave y expresiones y notifique a un ser humano si ha obtenido un resultado. El *software* comercial actual no es muy fiable a menos que primero se haya entrenado para hacerse a la voz del usuario. Pero un nivel de error que sería intolerable para usar un ordenador con el fin de dictar es más que adecuado para captar palabras clave de una conversación. Y el *software* está mejorando.

Los ordenadores trabajan barato. Si damos por hecho que el estadounidense medio pasa media hora al día en el teléfono (un número creado *grosso modo* realizando la media entre las dos horas de los adolescentes y diez minutos del resto), el resultado es, como media, seis millones de conversaciones telefónicas en un tiempo concreto. Aprovechando las maravillas de la producción masiva, debería de ser posible producir ordenadores suficientes dedicados a manejar todo eso por menos de mil millones de dólares. Y se está volviendo más barato cada año.

Todo teléfono de Estados Unidos.

Una digresión legal: mis instrucciones para los malos

Las agencias de ejecución de la ley todavía tienen que conseguir órdenes judiciales para todas esas escuchas; por muy amigables que sean los tribunales, convencer a los jueces de que se necesita pinchar todo teléfono en el país, incluido el suyo, podría ser un problema.

O quizás no. Una escucha informática no es realmente una invasión de la privacidad: nadie está escuchando. ¿Por qué debería exigir una orden de registro? Si fuera un abogado que trabaja para el FBI y estuviera frente a un juez amigable, argumentaría que una escucha informática es lo más equivalente a un registro de llamadas salientes,

que mantiene un registro de quién llama a quién y no necesita ahora mismo una orden. La escucha solo asciende al nivel de un registro cuando un humano escucha la conversación grabada. Antes de hacerlo, el ser humano irá, por supuesto, a un juez, le ofrecerá el informe informático con las palabras clave y expresiones detectadas y usará esa prueba para obtener una orden. Así, la ejecución de la ley será libre de pinchar todos nuestros teléfonos sin requerir permiso del sistema judicial, hasta que, por supuesto, encuentre pruebas de que estamos haciendo algo malo. Si no es así, solo un ordenador oirá nuestras palabras, así que ¿por qué preocuparnos? ¿Qué tenemos que ocultar?

CARNÉS DE IDENTIDAD VIVIENTES

Tras el ataque al World Trade Center ha habido presión política para establecer un sistema nacional de carnés de identidad; actualmente (definido por cuando estoy escribiendo, no cuando lo leas) no está claro si triunfará. A la larga, no importará mucho. Cada uno de nosotros ya tiene una variedad de tarjetas identificativas incorporadas: rostro, huellas dactilares, patrón de retina, ADN. Dada la tecnología adecuada para leer esa información, una tarjeta en papel es superflua.

En las poblaciones de baja densidad, el rostro solo ya es suficiente. Nadie necesita pedir identificación a un vecino porque ya todo el mundo conoce a todo el mundo.

Ese sistema colapsa en la gran ciudad porque no estamos equipados para almacenar y buscar un millón de caras. Pero podríamos estarlo. El *software* de reconocimiento facial existe y está mejorando. No hay razón técnica para que, en algún momento bastante cercano, alguien, probablemente la ejecución de la ley, no pueda compilar una base de datos que contenga todas las caras del país. Dirige la cámara a alguien y lee su nombre, edad, ciudadanía, historial delictivo y lo demás que esté en la base.

Las caras son una forma imperfecta de identificación, ya que hay formas de cambiar tu apariencia. Las huellas dactilares son mejores. Ya existen dispositivos comerciales para reconocer huellas dactilares, usados para controlar el acceso a los ordenadores portátiles. No sé lo

cerca que estamos de un lector de huellas dactilares unido a un sistema de clasificación, pero no parece un problema inherentemente difícil. Tampoco lo parece el uso equivalente de un escáner de patrones de retina. El reconocimiento barato del ADN está un poco más lejos, pero también ahí la tecnología ha estado progresando rápidamente.

Podríamos hacer leyes prohibiendo que los cuerpos de ejecución de la ley compilen y usen esas bases de datos, pero no parece probable que lo hagamos, dada la utilidad obvia de la tecnología para el trabajo que queremos que hagan. Incluso si lo prohibiéramos, ejecutar la prohibición contra la ejecución de la ley y el resto sería difícil. Cuando se montó el sistema de la Seguridad Social, la legislación prohibió explícitamente el uso del número de la Seguridad Social como identificador nacional. Sin embargo, el Gobierno federal y mucha otra gente normalmente te lo piden. Incluso si no hay una base de datos nacional de caras oficial, cada departamento de policía tendrá su propia colección de caras que le interesen. Si expandir esa colección es barato (y lo será), el «interés» se volverá una exigencia cada vez más débil. Y no hay nada que evite que los diferentes departamentos de policía hablen entre ellos.

LA OBSOLESCENCIA DEL DERECHO PENAL

Unos pocos capítulos atrás planteé la cuestión de si el acceso no autorizado a un ordenador debería ser tratado como responsabilidad civil o un delito. Ahora es hora de volver a ese asunto en un contexto más amplio.

La mayor parte de nosotros pensamos que la ejecución de la ley es casi completamente un terreno del Gobierno. De hecho, no lo es y, que yo sepa, nunca lo ha sido[76]. En EE.UU., el empleo total en disuasión de delitos privados (guardias de seguridad, instaladores de alarmas antirrobo y similares) ha sido desde hace mucho mayor que el de la ejecución de la ley. Capturar y procesar a los delincuentes lo hacen sobre todo los agentes del Gobierno, pero eso es solo porque el delito es definido como el tipo particular de falta que el Gobierno procesa. La

[76] Aunque la China Imperial podría haberse acercado. Véase Boddle y Morrid, 1973.

misma acción (matar a tu mujer, por ejemplo) puede ser procesada o por el Estado como un crimen o por partes privadas como responsabilidad civil, como O. J. Simpson descubrió.

Este hecho sugiere que podríamos no necesitar el derecho penal. Quizás podríamos apañarnos, incluso apañárnoslas mejor, con un sistema en que todas las acciones incorrectas las procesaran la víctima o los agentes de la víctima de forma privada. Esos sistemas han existido en el pasado. Podrían hacerlo de nuevo.

Una breve digresión temporal

Piensa, para uno de mis ejemplos favoritos, en el procesamiento penal en la Inglaterra del siglo XVIII. Sobre el papel, su sistema legal realizaba la misma distinción entre penal y responsabilidad civil como hace el nuestro. Lo penal era un delito contra la Corona: el caso era *Rex contra Friedman*[77].

La Corona poseía el caso, pero no lo procesó. Inglaterra en el siglo XVIII no tenía policía como entendemos la palabra: no había profesionales contratados por el Gobierno para atrapar y condenar a delincuentes. Había guardia, a veces sin sueldo, con poder para arrestar, pero deducir a quién arrestar no era parte de la descripción de su trabajo. La situación no cambió hasta la década de 1830, cuando Robert Peel creó la primera fuerza policial inglesa.

No solo no había policía, tampoco había fiscales públicos; el equivalente a fiscal del distrito del sistema estadounidense moderno no existió en Inglaterra hasta la década de 1870, aunque durante algunas décadas anteriores a eso los agentes de policía funcionaban como fiscales *de facto*. Sin policía ni fiscales públicos, el procesamiento de los delitos era necesariamente privado. La noma legal era que cualquier inglés podía procesar cualquier delito. En la práctica, el procesamiento lo llevaba usualmente la víctima o su agente.

---

[77] Friedman, 1995, en http://www.daviddfriedman.com/Academic/England18thc./England18thc.html.

Esto plantea un rompecabezas obvio. Cuando demando a alguien por responsabilidad civil, tengo la esperanza de ganar y que se me paguen daños, con suerte más que suficiente para cubrir mis facturas legales. Un fiscal privado bajo la ley penal no tenía ese incentivo. Si obtenía una condena, el delincuente sería colgado, deportado, se le permitiría engrosar en los servicios armados o sería perdonado, ninguna de las cuales ponía ningún dinero en el bolsillo del que dirige el procesamiento. Así que ¿por qué se iba a molestar nadie en llevar a cabo el proceso?

Una respuesta es que la víctima lo ejecutaba para evitar, no los delitos en general, sino los delitos contra su persona. Eso tiene sentido si es un habitual, como el propietario de una tienda o fábrica con continuo riesgo de ladrones. Cuelga a uno y los otros captarán el mensaje. Por eso, incluso hoy, en un sistema en que el procesamiento es completamente público, al menos nominalmente, los grandes almacenes tienen carteles anunciando que procesan a los ladrones. Seguramente por eso Intel procesó a Randy Schwartz.

La mayoría de las víctimas potenciales no son habituales. Para ellos, al inglés del siglo XVIII se le ocurrió una ingeniosa solución: sociedades para el procesamiento de delincuentes. Había miles de ellas. Los miembros de cada una contribuían con una pequeña suma a un fondo común, disponible para pagar el coste de procesar un delito cometido contra cualquier miembro de la sociedad. Los nombres de los miembros se publicaban en el periódico para que los leyeran los delincuentes. Las víctimas potenciales se comprometían así a procesar. Habían convertido la disuasión en un bien privado.

Ese tipo de instituciones se acabó abandonando. Una posible explicación es que, para que funcionara, los delincuentes tenían que conocer a sus víctimas, al menos lo bastante bien para saber si la víctima tenía fama de procesar o era un miembro de una sociedad que procesaba. A medida que Inglaterra se volvió cada vez más urbanizada, el delito se volvió cada vez más anónimo. No servía unirse a estas asociaciones y publicar tu nombre en el periódico local si el ladrón no conocía tu nombre. Otra posible explicación, argumentada por algunos académicos, es que la policía se introdujo como solución a otros problemas: quizás reformar a los pobres, quizás proporcionar un

Gobierno con la capacidad de asegurarse de que la Revolución Francesa, o algo similar, no sucediera en Inglaterra[78].

Hacia el pasado

Una consecuencia de la tecnología de procesamiento de la información moderna es el fin del anonimato, al menos en el espacio real. La información pública sobre ti es ahora verdaderamente pública; no solo está ahí fuera, cualquiera que la quiera puede encontrarla. En un capítulo anterior, lo discutí en el contexto de la privacidad. La privacidad a través de la oscuridad ya no es una opción. Ahora podemos ver una consecuencia diferente. En el siglo XIX, las grandes ciudades hacían anónimas a las víctimas. Ahora que nadie es ya anónimo, volvemos al siglo XVIII.

Piensa en nuestra anterior discusión sobre cómo manejar el acceso no autorizado a los ordenadores. Un problema de usar el derecho de responsabilidad civil es el incentivo inadecuado para procesar, ya que el *hacker*aleatorio podría no ser capaz de pagar una suma lo bastante grande en daños y perjuicios para cubrir el coste de encontrarlo y denunciarlo. Ese problema se solucionó hace doscientos cincuenta años. Bajo la ley penal no había daños y perjuicios que recaudar, así que los ingleses del siglo XVIII encontraron un incentivo diferente: la disuasión privada.

Piensa en la versión en línea de una sociedad para el procesamiento de delincuentes. Los suscriptores pagan una tasa anual en intercambio por la cual se les garantizan servicios de procesamiento si alguien accede a su ordenador de formas que les impongan costes. Los nombres de los suscriptores y sus direcciones IP se publican en una página web, para que los *hackers* prudentes los lean y eviten. Si el beneficio de la disuasión vale el coste, debería haber muchos clientes. Si no lo es, ¿por qué proporcionar disuasión a expensas de los contribuyentes?

---

[78] Para un ensayo que argumenta que las instituciones existentes estaban lidiando adecuadamente con los problemas de la urbanización y que explica el cambio a la política pública en otros términos, véase Davies, 2002.

Queda un problema. Bajo el derecho de responsabilidad civil ordinario, la pena es el daño realizado o la cantidad más grande que pueda pagar el infractor, la que sea menor. Si los intrusos informáticos son difíciles de encontrar, esa pena podría no ser adecuada para disuadirlos. Una de cada diez veces, el intruso debe pagar por el daño si puede. Las otras nueve veces sale libre.

El derecho penal resuelve ese problema permitiendo penas mayores, a veces mucho mayores, que el daño hecho, compensando así el factor de que solo se coge, condena y castiga a una fracción de los infractores. Los daños punitivos en el derecho de responsabilidad civil alcanzan el mismo efecto. Pero los daños punitivos están limitados a los activos del infractor, y el castigo penal no: el derecho penal puede imponer castigos no monetarios como el encarcelamiento.

Así que tenemos dos posibilidades de ejecución privada de normas legales contra el acceso no autorizado. Una es usar el derecho de responsabilidad civil ordinario, con disuasión privada como incentivo para procesar. Esto funciona siempre que los activos de los infractores sean lo bastante grandes como para que dirigir una demanda civil sea un castigo adecuado para disuadir la mayor parte de las infracciones. La otra es volver completamente al siglo XVIII: el procesamiento privado con penas penales.

He discutido los problemas con el procesamiento privado: ¿cuáles son las ventajas? La principal es la ventaja que la empresa privada normalmente posee sobre la pública. Los propietarios de una empresa de procesamiento en línea están vendiendo un servicio a sus clientes en un mercado competitivo. Cuanto mejor hagan su trabajo, más probable es que ganen dinero. Si los costes son elevados y la calidad, baja, no tendrán la opción de ser rescatados por los contribuyentes.

El argumento se aplica a más que la defensa de ordenadores contra intrusos no deseados. La tecnología de procesamiento de información elimina el anonimato que creó la urbanización; en ese respecto, al menos, nos pone de nuevo en pueblos. Hacer eso elimina lo que era posiblemente la razón principal para el cambio del procesamiento privado al público. De todo delito.

Ejecución privada en línea

Mi interés en el futuro de la ejecución privada en línea estaba en parte inspirado por la historia y teoría económica, en parte por noticias sobre los delincuentes atrapados por sus víctimas que usaban Internet para coordinar sus esfuerzos: control de delitos de fuente abierta, como discutimos en un capítulo anterior.

Estas historias sugieren otra forma de que la tecnología moderna pueda hacer la ejecución legal privada más práctica de lo que ha sido en el pasado reciente. Muchos delitos involucran a un solo delincuente, pero a múltiples víctimas. Cada víctima posee razones, prácticas y morales, para querer que se coja al delincuente, pero ninguna puede hacer el trabajo por su cuenta. Internet, reduciendo drásticamente el coste de encontrar a otras víctimas y coordinarlas, ayuda a resolver ese problema.

PARTE 5

BIOTECNOLOGÍA

TRECE

REPRODUCCIÓN HUMANA

A lo largo de la mayor parte del siglo pasado, la tecnología reproductiva mejorada ha consistido en gran parte de maneras mejores para no reproducirse. La mejora en los anticonceptivos ha venido acompañada de cambios impresionantes en los patrones de apareamiento humano: un declive pronunciado del matrimonio tradicional, un incremento correspondiente en el sexo extramatrimonial y, quizás algo sorprendente, tasas extraordinariamente altas de alumbramientos fuera del matrimonio. Mientras que las consecuencias a largo plazo de la anticoncepción fiable seguirán representando un papel durante las siguientes décadas, no las discutiremos aquí. Este capítulo trata de desarrollos más recientes en la tecnología de la reproducción humana.

CONSTRUYENDO MEJORES BEBÉS

La eugenesia, la idea de mejorar la especie humana mediante reproducción selectiva, fue apoyada por mucha gente a finales del siglo XIX y principios del XX[79]. Actualmente está considerada, en la retórica de la controversia, solo un poco por encima del nazismo. Casi cualquier tecnología reproductiva capaz de beneficiar a generaciones futuras está en riesgo de ser atacada como «eugenesia» por sus oponentes.

Ese argumento confunde, a veces deliberadamente, dos maneras muy diferentes de alcanzar objetivos similares. Una es tratar a los seres humanos como perros del espectáculo o caballos de carreras: que alguien, probablemente el Estado, decida quiénes se pueden reproducir para mejorar la raza. Una política así implica forzar a la gente que

---

[79] Incluyendo a George Bernard Shaw, H. G.Wells, John Maynard Keynes, Harold Laski, y a los Webbs en la izquierda, y Winston Churchill en la derecha. Sus oponentes incluían a G. K.Chesterton, la Iglesia Católica, y a JosiahWedgewood, un miembro del Parlamento libertario radical (Ridley, 1999, pp. 292–295).

quiere tener hijos a no tenerlos y, quizás, forzar a la gente que no quiere tenerlos a tenerlos. Además, impone los deseos del planificador eugénico sobre todos; no hay razón para dar por hecho que el resultado sería una mejora desde el punto de vista del resto de nosotros. Un Estado prudente podría decidir que la sumisión, obediencia a la autoridad y características similares eran para lo que quería la reproducción.

Eugénica libertaria

La alternativa es lo que considero eugenesia libertaria. La descripción más temprana que conozco se encuentra en una novela de ciencia ficción, *Beyond This Horizon*, de Robert Heinlein, posiblemente uno de los escritores de ciencia ficción más capaces e innovadores del siglo XX.

En la historia de Heinlein, las parejas utilizan la tecnología genética para controlar cuál de los niños que podrían producir producen. Con la ayuda de consejo experto, seleccionan entre los óvulos producidos por la esposa y el esperma producido por el marido la combinación particular de óvulo y esperma que producirá el niño que más quieren tener, el que no lleva el gen del marido de un corazón enfermo o el de la esposa de mala circulación, pero sí lleva el de la buena coordinación del marido y la habilidad musical de la esposa. Cada pareja obtiene su propio hijo, aunque las características que los padres no quieren que tengan sus hijos gradualmente se eliminan de la reserva genética. Ya que la decisión la toma cada pareja para sus propios hijos, y no alguien para todos, debería de mantener un alto nivel de diversidad genética; padres diferentes querrán cosas diferentes. Y ya que se puede confiar en que los padres, a diferencia de los planificadores del Estado, se preocupen mucho sobre el bienestar de sus hijos, la tecnología debería usarse sobre todo para mejorar la próxima generación, no para explotarla.

La tecnología de Heinlein no existe, pero su resultado, en crudo, sí. El método actual, más primitivo, es que una mujer conciba, obtenga células fetales extrayendo líquido amniótico («amniocentesis»), haga que comprueben las células para ver si llevan algún defecto genérico

serio (en particular, la copia extra del cromosoma 21 que produce el síndrome de Down) y aborte el feto si es así[80].

Una versión que elimina los costes emocionales (algunos dirían morales) del aborto está empezando a usarse. Obtén óvulos de la que tiene intención de ser madre, esperma del que desea ser padre. Fertilízalos *in vitro* (fuera del cuerpo de la madre). Deja que crezcan los óvulos fertilizados hasta que el embrión tenga ocho células. Extrae una célula, algo que en ese punto se puede hacer sin dañar al resto. Analiza sus genes. Selecciona de los óvulos fertilizados uno que no lleve ningún defecto genético serio de los que están intentando evitar. Implanta de nuevo ese óvulo a la madre.

En el presente hay dos limitaciones principales en este proceso. La primera es que la fertilización *in vitro* (FIV) todavía es un proceso difícil y caro. La segunda es que la prueba genética es una tecnología nueva, así que solo un pequeño número de características genéticas pueden identificarse en la célula. Algunas enfermedades genéticas, sí; la habilidad musical o la inteligencia, no. Sin embargo, el uso de la FIV está aumentando; en la cohorte de mujeres danesas nacidas en 1978, el 6% de los bebés se produjeron con la ayuda de tecnologías reproductivas artificiales como la FIV. Dadas las tasas de progreso actuales, es probable que la segunda limitación se reduzca rápidamente durante los próximos diez o veinte años. Entonces estaremos en un mundo en que al menos algunas personas sean capaces de producir deliberadamente los niños «mejores y más brillantes» de todos lo que podrían haber tenido. Esa habilidad se incrementará enormemente cuando y si obtenemos la habilidad de determinar la estructura genética del óvulo y el esperma antes de que se combinen, con lo que se incrementaría enormemente la posibilidad de alternativas entre las que puede elegir el progenitor[81].

---

80 Una forma todavía más cruda, exponiendo a niños enfermizos, precede a Heinlein varios miles de años.

81 El problema obvio es que examinando un óvulo o esperma es probable que lo dañemos. La ingeniosa solución de Heinlein (no sé si era invención propia o no) era aprovechar el hecho de que cada esperma contiene la mitad de los genes paternos, al haberse producido por un proceso de división de una célula que contenía todos ellos. Todo el genotipo se encuentra reproducido en cada célula, así que podemos, dadas las tecnologías de cartografía genética adecuadamente avanzadas (que ahora existen y pronto serán baratas) conseguirlo analizando destructivamente unas pocas de ellas. Entonces analizamos una

Hasta ahora hemos estado considerando una tecnología reproductiva que ya existe, aunque en un nivel muy primitivo; seleccionar entre los óvulos fertilizados producidos por una sola pareja. Pasamos a unas tecnologías más nuevas. La primera que ha recibido la mayor parte de la atención es la *clonación*, producir un individuo que es genéticamente idéntico a otro[82]. Una forma de clonar es natural y muy común; los gemelos idénticos son genéticamente idénticos el uno al otro. El mismo efecto se ha producido artificialmente en la cría animal: obtén un solo óvulo fertilizado, a partir de él produce múltiples óvulos fertilizados e implántalos para producir múltiple descendencia genéticamente idéntica. En la agricultura, clonar para reproducir variedades particularmente deseables de vides o manzanos (injertar) es una tecnología que se ha practicado desde hace más de dos mil años.

La forma de clonar que se ha vuelto controvertida recientemente comienza en cambio con una célula de un animal adulto y la usa para producir un bebé que es el gemelo idéntico de ese adulto. Mucha de la hostilidad inicial contra la tecnología parecía estar enraizada en la extraña creencia de que clonar duplica a un adulto, que, tras ser clonado, un yo puede terminar de escribir este capítulo mientras el otro mete a mis hijos en la cama. Así no es cómo funciona la clonación, aunque discutiremos algo muy similar en un capítulo posterior, en el que la copia será de silicio en vez de carbono.

Otra tecnología, un poco más lejana en el futuro, es la ingeniería genética. Si supiéramos lo bastante sobre cómo funcionan los genes y cómo manipularlos, podría ser posible tomar material genético de espermatozoides, óvulos o células adultas aportadas por dos o más individuos y combinarlas, produciendo un solo individuo con una selección de genes a medida.

---

mitad de la división, destruyéndola en el proceso, y deducimos lo que debía de haber en la otra mitad. Ahora conocemos el contenido genético de un esperma que no hemos examinado y, por tanto, no hemos dañado. Un proceso análogo podría aplicarse a los óvulos. En ambos casos, probablemente se necesita que el estadio final en la producción de óvulos o esperma ocurra fuera del cuerpo, donde podemos seguir lo que está pasando.

[82] Estrictamente hablando, los clones creados de una célula adulta son idénticos solo en el ADN nuclear; el ADN mitocondrial, que sale del óvulo, es diferente a menos que el óvulo en que el núcleo está inserto sea o del mismo individuo que la célula o un antepasado maternal de ese individuo (madre, madre de la madre...) o alguien que comparta un antepasado en la línea materna directa (hija de la madre, hija de la madre de la madre...). En el resto de la discusión ignoraré esta complicación en aras de la simplicidad.

La reproducción sexual ya combina genes de nuestros padres en nosotros. La ingeniería genética nos dejaría elegir qué genes vinieron de cuáles, en vez de aceptar una selección aleatoria. También nos permitiría combinar genes de más de dos individuos sin necesitar múltiples generaciones para hacerlo, así como unir genes útiles de otras especies. Las versiones primitivas de la tecnología ya se han usado exitosamente para insertar genes de una especie de planta o animal en otra.

Otra posibilidad es crear genes artificiales, quizás todo un cromosoma adicional[83]. Estos genes se designarían para hacer cosas que nosotros quisiéramos dentro de nuestras células (evitar el envejecimiento, digamos, o luchar contra el SIDA), pero que no ha hecho ningún gen existente. Construirlos sería un proyecto en la intersección de la biotecnología y la nanotecnología.

Las tecnologías actuales y del futuro cercano que controlen qué tipo de hijos tenemos dependen de la FIV, una tecnología desarrollada originariamente para hacer posible que mujeres que de lo contrario serían estériles tengan hijos. También hace posible la clonación artificial de óvulos, dejando que se divida el óvulo fertilizado y luego separándolo en dos. Esto hace posible la clonación de células adultas, reemplazando el núcleo de un óvulo fertilizado por un núcleo de una célula adulta, y aún podría hacer posible la ingeniería genética y los genes artificiales. También ha hecho ya posible que las madres de alquiler tengan hijos producidos a partir de los óvulos fertilizados de otras mujeres.

Otras tecnologías nuevas podrían hacer posible la reproducción de un tipo distinto de padres no fértiles: las parejas del mismo sexo. Ahora una pareja de mujeres que deseen criar un niño puede, al menos en algunos estados federados, adoptar uno. Si no, una de las mujeres puede concebir un hijo usando esperma donado. Pero no pueden hacer lo que la mayoría de otras parejas que desean tener hijos hacen: producir un hijo que sea la descendencia genética de ambos. Lo más cercano que se puede conseguir con la tecnología tradicional es usar esperma donado por un padre o hermano de uno para inseminar al

[83] Lee Silver discute esta posibilidad en *Remaking Eden*.

otro, con lo que se produce un hijo que es, genéticamente hablando, la mitad de uno y un cuarto del otro.

Esa situación está cambiando. Se han desarrollado técnicas para producir esperma artificial que contenga material genético de una célula adulta. Ello podría posibilitar que en un futuro muy cercano dos mujeres produzcan un hijo que sea suyo en todos los sentidos. En algún momento una tecnología análoga podría hacer posible los óvulos artificiales, lo que permitiría que dos hombres, con la ayuda de un útero prestado, produzcan un hijo que es suyo en el mismo sentido[84].

CÓMO ACTUALIZAR EL DISEÑO DE UN CROMOSOMA

Si tu meta es manipular genéticamente a un ser humano, necesitas insertar un gen en cada célula relevante, o comenzar con un embrión de una sola célula.

Matt Ridley, *Genoma*, pág. 247 (traducción nuestra)

La ingeniería genética que hemos estado discutiendo se aplica a una sola célula, un óvulo fertilizado. Hacerlo es una forma elegantemente simple de cambiar las cosas, ya que las características modificadas de una sola célula se pasarán a cada célula del cuerpo construido a partir de esa célula y a cualquier nuevo cuerpo que provenga de ella. Por la misma razón, algunos encuentran aterradora la aplicación de esas tecnologías a los humanos, una forma de cambiar permanentemente al menos parte de la raza humana.

El término técnico es *ingeniería genética de la línea del germen*. Sorprendentemente, no es la única forma de modificar cosas vivientes

[84] En el caso de dos mujeres, si el niño es completamente suyo, debe de ser una hija, puesto que ninguna tiene un cromosoma Y para aportar. En el caso de dos hombres, podría ser o un hijo o una hija, puesto que el macho tiene un cromosoma X y un Y. Lee Silver (1998) describe dos tecnologías que podrían usarse para producir hijos para parejas del mismo sexo. Sin embargo, cada una da lugar a un niño que es solo un 25% el producto de cada progenitor genéticamente. En un caso, el niño es una quimera (un organismo producido fusionando dos óvulos fertilizados, con lo que da lugar a un individuo la mitad de cuyas células proviene de un óvulo y la mitad, del otro). En el otro caso el niño es, genéticamente hablando, el nieto de la pareja: se ha abortado la generación que interviene y se han recogido las células necesarias para producir un óvulo fertilizado.

cambiando sus genes. La alternativa es cambiar genes de las células de un organismo ya existente. Ello plantea un problema obvio. Cambiar los genes en una sola célula es un procedimiento difícil y arriesgado. Un solo cuerpo humano contiene un billón de células[85]. ¿Cómo se pueden cambiar las suficientes para que importe el cambio?

Ese problema se solucionó hace mucho tiempo, y no fueron los humanos quienes lo solucionaron.

Los virus se reproducen secuestrando el mecanismo de una célula, modificándolo y usándolo para producir más virus. Ya que los virus nos secuestran, parece justo que los secuestremos.

Un retrovirus contiene un mensaje escrito en ARN que dice, en esencia, «Haz una copia de mí y cósela en tu cromosoma». Todo lo que necesita hacer un terapeuta genético es coger un retrovirus, cortar unos pocos de sus genes..., ponerlos en un gen humano e infectar al paciente con ellos. El virus va al trabajo insertando el gen en las células del cuerpo y tienes una persona genéticamente modificada.

Ridley, *Genoma*, pág. 247

Esta forma de ingeniería genética ya se ha usado para combatir la inmunodeficiencia combinada grave (IDCG), la enfermedad genética responsable de que los cuerpos de los niños sean incapaces de defenderse contra la infección[86]. Solía pasar que estos niños pudieran ser mantenidos con vida solo en un ambiente estéril y que murieran jóvenes. Más tarde se descubrió un método para tratar la enfermedad mediante inyecciones mensuales de la proteína que los genes defectuosos no conseguían fabricar. Actualmente, esa solución se combina con terapia genética que repara algunos de los genes defectuosos y así reduce la dependencia de la víctima a la proteína inyectada. Se están desarrollando curas similares para una variedad de otras enfermedades.

---

85 Diferentes fuentes dan estimaciones diferentes: voy a utilizar cien billones, aquí y más adelante, ya que es un número lo bastante redondo.

86 Uno niño así se volvió famoso como «niño burbuja». Véase http://www.texaschildrenshospital.org/Web/50Years/patients david.htm.

La IDCG es una enfermedad poco común. El cáncer, por otra parte, es una de las causas de muerte principales en las sociedades modernas, solo tras enfermedades cardiacas y se espera que pronto las adelante. Y el cáncer es una enfermedad genética.

Mi desarrollo de un óvulo fertilizado a un adulto fue posible por la división celular, comenzando con una única célula. Así es el proceso de curar heridas construyendo un nuevo tejido para reemplazar el antiguo. Una vez llego a mi tamaño completo, la mayoría de esas células deben parar de dividirse, ya que de lo contrario seguiré creciendo. Las células vienen con mecanismos que las hagan dividirse (oncogenes) que se desconectan cuando ya no es necesaria la división. Vienen dotados de mecanismos adicionales para que dejen de dividirse, en caso de que el oncogén se quede atascado en la división. Y, solo por seguridad, tienen un tercer mecanismo para hacer que la célula se autodestruya si los dos primeros fallan.

La mutación cambia a los genes. Si suceden los suficientes cambios en la misma célula para hacer fallar los tres mecanismos, tienes cáncer; esa es, al menos, la teoría actual. Que las tres cosas distintas se rompan en la misma célula es, por supuesto, muy improbable. Pero con cien billones de células, pueden pasar incluso cosas muy improbables, lo que sugiere una táctica posible para curar el cáncer. Modifica genéticamente las células cancerígenas de forma que arregles al menos una de las tres cosas que no funcionan en ellas. Si arreglas una de las dos primeras, las células cancerígenas dejan de dividirse. Si arreglas la tercera, mueren.

La posibilidad de actualizar células con nuevos genes también sugiere una posibilidad tentadora y preocupante para la ejecución legal de alta tecnología. Supón que deducimos que algunas de las causas del comportamiento delictivo son genéticas; quizás haya un gen, más probablemente un conjunto de genes, de psicopatía. En vez de condenar a un delincuente a ser encarcelado, lo condenamos a que corrija sus genes: una versión nueva de alta tecnología del viejo sueño de reformar a los delincuentes en vez de disuadirlos.

Cuando hemos terminado de alterar algunos de los genes en cada célula de su cuerpo (estoy dando por hecho una versión más avanzada

de la tecnología que la que tenemos actualmente), ¿es todavía la misma persona? ¿Lo hemos reformado o reemplazado?

Quizás Huxley acertó

Hasta ahora he estado discutiendo formas de cambiar cómo es la gente cambiando sus genes. Otra posibilidad es cambiar su ambiente, su primer ambiente. Ahora hay pruebas de que las características sutiles del ambiente prenatal, el útero de la madre, tiene efectos significativos e interesantes sobre cómo acaba siendo el ocupante.

Mira una de tus manos y compara la longitud del primer y tercer dedo. Como media, cuanto más grande sea la longitud relativa del tercer dedo, mayor es el nivel de testosterona (y menor el nivel de estrógeno en el útero que ocupaste). La longitud de los dedos no importa mucho, pero la longitud del dedo no es todo lo afectado: la longitud relativa de esos dos dedos también es correlativa a los resultados relativos de los niños en las pruebas de conocimientos matemáticos y alfabetización[87]. Hace mucho que se ha observado que, como media, los hombres parecen ser relativamente mejores en aprendizaje matemático, las mujeres en el verbal. Aparentemente la diferencia se debe, al menos en parte, a sus diferentes ambientes del útero. No solo un útero con un feto masculino tiene, como media, un nivel mayor de testosterona que uno con un feto femenino, sino que entre los masculinos o femeninos el nivel de testosterona se correlaciona con las capacidades relativas matemáticas y verbales.

En *Un mundo feliz*, Huxley describió una distopia futura en que el Estado producía diferentes tipos de personas para propósitos distintos, cada una diseñada para ser buena en y estar contenta con un papel particular en la vida. Lo hacían controlando no lo genes, sino la química uterina, usando úteros artificiales para ese fin. Podría haber acertado.

---

[87] Las pruebas fueron los Standardized Assessment Tests, que se realizan en Reino Unido a los 7 años. Muchas noticias los confundieron con el examen SAT de EE.UU., que es el que se realiza a los estudiantes que echan la solicitud para entrar a una universidad. Un resumen del artículo original se encuentra en http://www.ingentaconnect.com/content/bpsoc/bjp/2008/00000099/00000001/art00005.

¿POR QUÉ MOLESTARSE?

Las nuevas tecnologías hacen posible la realización de tareas nuevas; queda la cuestión de si merece la pena hacerlas. En el caso de la tecnología reproductiva, la fuerza conductora inicial, todavía importante, era el deseo de que la gente tenga sus propios hijos. De ahí obtenemos la FIV y el uso de madres de alquiler para permitir que una madre incapaz de llevar a término su feto tenga a alguien que lo haga por ella. El deseo de tener tus propios hijos también proporciona un posible incentivo para la clonación: permitir que una pareja incapaz de producir un hijo de ambos —porque uno de ellos no es fértil— produzca en cambio un hijo que es un gemelo idéntico de uno y que las tecnologías permitan reproducirse a las parejas del mismo sexo.

Un segundo motivo, cada vez más importante, es el deseo de tener hijos mejores. En los primeros estadios de la tecnología, esto significa evitar la catástrofe de defectos genéticos serios. A medida que la tecnología mejora, abre la posibilidad de eliminar efectos menos serios (el riesgo de un corazón enfermo, digamos, que parece ser en parte genético, o el alcoholismo, que podría serlo) y seleccionar en favor de las características deseables. Los padres quieren que sus hijos sean felices, sanos, inteligentes, fuertes, hermosos. Esas tecnologías proporcionan maneras de mejorar las posibilidades.

Uno puede imaginar usos para la tecnología encaminados a otros propósitos. Un Gobierno dictatorial podría intentar aplicar la tecnología a la población entera, para hacer desaparecer alguna característica, digamos la agresividad o resistencia a la autoridad. Un Gobierno menos ambicioso podría usar la clonación para producir múltiples copias del soldado perfecto, o policía secreto, o investigador científico, o dictador, aunque múltiples dictadores idénticos podría ser complicarse la vida.

Estos marcos hipotéticos son más plausibles como argumentos de película que como políticas. Se necesitan unos veinte años para producir un humano adulto; pocos Gobiernos del mundo real pueden permitirse planificar para un futuro tan lejano. Y mientras que un clon será genéticamente idéntico al donante, su ambiente no lo será, así que aunque la clonación produce un resultado más predecible que la

reproducción sexual, está lejos de ser perfectamente predecible[88]. Obtener tus soldados, policía secreta, científicos o dictadores de la forma tradicional tiene la ventaja de dejarte seleccionarles a partir de una gran población de personas ya adultas y observables.

Otro argumento contra la idea es que si fuera una estrategia atractiva para un Estado dictatorial, ya debería haber sucedido. La cría selectiva de animales es una tecnología muy vieja. Aun así no conozco ninguna sociedad pasada que hiciera ningún intento serio a gran escala de cría selectiva de humanos para producirlos según los rasgos deseados por los que mandan[89]. En tanto que hemos observado la cría selectiva de humanos, ha sido a nivel individual o familiar, gente que elige a sus parejas para ellos o sus hijos en parte de acuerdo con qué tipo de hijos creen que ayudará a producir esa pareja.

Un problema más serio es la explotación de niños clonados a gran escala. En una versión a veces ofrecida como argumento contra la clonación de humanos, un adulto produce un clon de sí mismo para desmembrarlo en partes corporales que se usen en trasplantes futuros. Un problema obvio con ese marco hipotético es que incluso si la clonación fuera ilegal, el desmembramiento no lo sería, en EE.UU. actualmente o en cualquier sociedad razonablemente similar. Pero uno puede imaginarse una sociedad futura en la que lo fuera. Por otra parte, el proceso de nuevo tiene un lapso de tiempo sustancial, y se vuelve cada vez menos útil a medida que la tecnología médica mejorada reduce los problemas de rechazo de trasplantes.

Sin embargo, ha habido al menos un caso en el mundo real remotamente análogo a este. Observarlo sugiere que producir un ser humano, al menos en parte, para proporcionar tejido para trasplantes pudiera no ser una idea horrorosa después de todo. En 1988, a Anissa Ayala, entonces una estudiante de segundo año de instituto, se le diagnosticó una forma de leucemia con progreso lento pero en última

[88] Este fue uno de los asuntos subyacentes en *Los niños de Brasil*, 1991, una novela sobre un proyecto secreto para producir múltiples clones de Adolf Hitler, de la que más tarde se hizo una exitosa película.

[89] Dos ejemplos posibles de proyectos a pequeña escala que siguen este hilo es el intento fallido del emperador Federico Guillermo de Prusia de juntar a hombres altos con mujeres altas para producir reclutas altos para su regimiento de «Gigantes de Potsdam», y los intentos de Hitler de hacer que se reprodujeran los mejores hombres y mujeres alemanes.

instancia mortal. Su única esperanza era un tratamiento que mataría todas sus células madre existentes en la sangre y reemplazarlas por un transplante de un donante compatible. Las posibilidades de que un donante aleatorio fuera compatible eran de una entre veinte mil.

Sus padres pasaron dos años buscando sin éxito un donante compatible, luego decidieron intentar producir uno. Las posibilidades no eran buenas. Un segundo hijo solo tendría un 25% de posibilidades de compatibilidad. Incluso con un donante compatible, el procedimiento tendría una probabilidad de supervivencia de solo el 70%. La madre ya tenía cuarenta y dos años; el padre se había hecho la vasectomía. La alternativa era peor: los padres de Anissa se la jugaron. La vasectomía se invirtió con éxito. Su segunda hija, Marissa, nació. Y fue compatible. Catorce meses más tarde, donó la médula ósea que, como lo expresó cinco años más tarde en una entrevista para la televisión, salvó la vida de su hermana.

Marissa fue producida por métodos convencionales; el elemento controvertido, condenado estrepitosamente por una variedad de bioéticos, fue producir un niño con la esperanza de que pudiera donar la médula ósea requerida para salvar a otro. Pero la clonación, si hubiera sido práctica, habría aumentado las posibilidades de que concuerden de 25% a 100%.

Para otro uso potencialmente controvertido de la clonación, piensa en los padres cuyo niño pequeño acaba de matarse en un accidente de coche. Los padres invierten mucho emocionalmente en sus hijos, no hijos en abstracto, sino en esta pequeña persona en particular a quien aman. Clonar les permitiría, en un sentido real pero incompleto, recuperarla, en forma de un segundo hijo muy idéntico al primero[90].

Razones para no hacerlo

No comparto tus principios, y exigiré que mueras por los míos.
La visión de Voltaire, revisada bioéticamente

---

90 A finales del 2004 se informó de un caso real (con un gato, no un bebé): http://www.cnn.com/2004/TECH/science/12/23/gen.us.clonedcat.ap/index.html.

Las tecnologías reproductivas (más recientemente, la clonación; antes, los anticonceptivos, la FIV y la inseminación artificial) han suscitado una oposición global. Una razón, la idea de que esta tecnología podría ser particularmente útil para un Estado dictatorial, ya la he descartado como implausible. Hay al menos otras tres.

La primera es el factor «puaj». Las nuevas tecnologías que tratan con cosas tan íntimas como la reproducción suscitan sentimientos extraños, antinaturales, y, para mucha gente, aterradores y desagradables. Era así con los anticonceptivos, era así para la FIV y la inseminación artificial, es así hasta un punto impactante con la clonación, y no hay duda en que será así para la ingeniería genética cuando y si podemos llevarla a cabo. Esa reacción podría ralentizar la introducción de nuevas tecnologías reproductivas, pero es improbable que las impida, siempre que esas tecnologías posibiliten que la gente haga cosas que desean hacer.

Una segunda razón es que las nuevas tecnologías normalmente no funcionan muy bien al principio. A juzgar por la experiencia que hasta ahora tenemos de clonar grandes mamíferos, si alguien intentara clonar a un humano mañana, se requerirían muchos intentos sin éxito para producir un niño vivo y ese niño podría sufrir una variedad de problemas. Este es un argumento sólido contra clonar a un ser humano hoy en día, pero se irá debilitando a medida que experimentos ulteriores de clonar otros mamíferos grandes produzcan cada vez más información sobre cómo hacerlo correctamente.

La razón final es la más interesante de todas. Es la posibilidad de que las decisiones reproductoras individuales pudieran tener consecuencias no intencionadas, quizás seriamente negativas.

¿Dónde han ido todas las mujeres?

Piensa en un ejemplo simple: la elección del sexo. A menudo, los padres tienen una preferencia sobre si quieren un niño o una niña. La tecnología más simple para darles lo que quieren (el infanticidio selectivo) ha estado en uso durante miles de años. Una alternativa menos costosa (el aborto selectivo) ya se está usando abundantemente

en algunas partes del mundo[91]. Y ahora tenemos formas de alterar sustancialmente las probabilidades de producir descendencia masculina o femenina mediante métodos más o menos drásticos[92]. A medida que esas técnicas se vuelvan más fiables y estén más disponibles, iremos hacia un mundo en el que los padres tengan un control casi completo sobre el sexo de la descendencia que produzca. ¿Cuáles serán las consecuencias?

Para la respuesta más extrema, piensa en la situación con la política de un solo hijo de China, impuesta en una sociedad donde las familias desean de fuerza al menos un hijo varón. El resultado es que una mayoría sustancial de los niños son varones; algunas estimaciones sugieren unos ciento veinte niños por cada cien niñas. Un efecto similar, pero más débil ha ocurrido en India, incluso sin restricción sobre el número de niños; las cifras recientes sugieren unos ciento siete niños de cada cien niñas. Con mejores tecnologías para la selección del sexo, la proporción sería mayor. Es probable que la consecuencia sea sociedades en que muchos hombres tengan problemas para encontrar a una mujer.

El problema podría corregirse por sí mismo: tras un lapso de tiempo. En una sociedad con una alta proporción de hombres frente a mujeres, las mujeres están en una posición de negociar muy fuerte, son capaces de elegir los compañeros y exigir términos favorables en el matrimonio[93]. Cuando esto se vaya viendo claro, aumentarán los beneficios de producir hijas. No tiene mucho sentido preservar el apellido teniendo un hijo si no puede encontrar una mujer dispuesta a producirte nietos. Una alta proporción de hombres frente a mujeres

---

[91] http://www.wikipedia.org/wiki/Sex-selective abortion; http://www.theworldjournal.com/forum/viewthread.php?tid=256; http://www.kit.nl/ils/exchange content/html/female infanticide - sexual he.asp; http://www.hsph.harvard.edu/rt21/medicalization/WEISS Sexselective. html; http://www.futurepundit.com/archives/002075.html.

[92] http://www.wikipedia.org/wiki/Sex-selective abortion; http://www.theworldjournal.com/forum/viewthread.php?tid=256; http://www.kit.nl/ils/exchange content/html/female infanticide - sexualhe.asp; http://www.hsph.harvard.edu/rt21/medicalization/WEISS Sexselective. html; http://www.futurepundit.com/archives/002075.html.

[93] Para una discusión de la economía relevante, véase Friedman, 1986, Capítulo21, en http://www.daviddfriedman.com/Academic/Price Theory/PThyChapter 21/PThy Chap 21.html.

también podría acabar en un cambio en los patrones de apareamiento hacia la dirección de la poliandría: dos o más maridos compartiendo a la misma mujer. Incluso sin cambios en las leyes matrimoniales, todavía existe la posibilidad de poliandría consecutiva. Una mujer se casa con un hombre, le produce un hijo, se divorcia y se casa con un segundo marido[94].

Genes de clase

¿Y las tecnologías que permiten que los padres escojan entre los niños que podrían tener, e incluso elijan añadir genes útiles, quizás artificiales, que ninguno de los padres lleva? Lee Silver, un genetista de ratones y autor de un fascinante libro sobre tecnología reproductiva[95], se preocupa de que el resultado a largo plazo pudiera ser una sociedad dividida en dos clases: generricos, los descendientes genéticamente superiores de gente que pudo permitirse usar las nuevas tecnologías para producir una descendencia superior, y genepobres.

Hay dos razones por las que no es probable que suceda. La primera es que las generaciones humanas son largas y el cambio tecnológico es rápido. Podríamos tener diez o veinte años en que la gente de mayor renta tenga oportunidades sustancialmente mejores de seleccionar a sus hijos. Después, la nueva tecnología, como muchas antiguas, probablemente se volverá lo bastante barata como para estar disponible para casi cualquiera que realmente la quiera. No hace tanto, después de todo, que la televisión era una tecnología nueva que se limitaba a la gente de dinero. Actualmente, alrededor de un 97% de familias estadounidenses por debajo del umbral de la pobreza poseen al menos una televisión en color.

La segunda razón es que el apareamiento humano no se da estrictamente dentro de la misma clase. Los ricos a veces se casan con las pobres y viceversa. Incluso sin matrimonio, si se cree que los ricos tienen genes superiores (como se creería tras una generación o dos del

[94] Dos discusiones ficticias interesantes de estos asuntos son Heinlein, 1966, y Schulman, 1983. El último describe un mundo con proporción de hombres frente a mujeres muy alta, en el que se llamaba a las mujeres a la prostitución temporal.

[95] Silver, 1998.

futuro hipotético de Lee Silver), es una razón de más para que menos mujeres ricas conciban hijos suyos, un patrón que, por muy ofensivo que resulte a las sensibilidades igualitarias, es históricamente común. Puesto en términos económicos, el esperma es un bien gratuito, por lo que proporciona una forma de bajo coste de obtener genes de alta cualidad para la descendencia de uno. Dudo de que lleguemos tan lejos, pero si lo hacemos, podemos confiar en que el patrón de apareamiento humano tradicional (monogamia suavizada por el adulterio) desdibuje cualquier frontera genética aguda entre clases sociales o económicas.

PARANDO EL RELOJ BIOLÓGICO

Todo lo que no está prohibido es obligatorio.

Señal sobre la entrada a la colonia de hormigas en *La leyenda del rey Arturo*

En nuestra sociedad, se supone que la gente no debería volverse activa sexualmente hasta que se vuelven adultos. En la práctica no funciona así, lo que lleva a problemas con los que cualquiera que lea periódicos, vea la televisión o se preocupes de sus propios hijos está familiarizado. El problema es que estamos físicamente preparados para reproducirnos antes de que lo estemos emocional o económicamente. Esto se ha vuelto cada vez más cierto a medida que ha ido cayendo la edad de la madurez física (unos dos años en el último siglo, probablemente como resultado de una nutrición mejorada). Con el progreso continuo de la ciencia médica, podríamos ser capaces de invertir ese cambio pronto.

Supón que una compañía farmacéutica anuncia un nuevo medicamento, uno que retrase la pubertad de forma segura en un año, o dos, o tres. Predigo que habrá una demanda considerable para ese producto. ¿Son culpables de maltrato los padres que retrasan artificialmente el desarrollo físico de sus hijas? ¿Pueden presionar los colegios a los padres para que den la medicación a los niños que estén a punto de alcanzar la pubertad, como muchos hacen ahora con otras formas de medicación diseñada para hacer que los niños se comporten más como los profesores quieren? Si los colegios lo exigen, ¿son

culpables de maltrato los padres que se niegan a retrasar artificialmente el desarrollo de sus hijos, o al menos estarán sujetos a las mismas presiones que los padres que hoy en día se niegan a dar a sus hijos el medicamento tranquilizante Ritalin?

Ahora que estamos en el tema, ¿y la aplicación de tecnología similar a otras especies? Los gatos son criaturas adorables, pero los gatitos son mucho más divertidos. Ojalá siguieran siendo gatitos un poco más de tiempo…

CATORCE

CUANTO MÁS SABES…

El capítulo anterior discutía cambios en lo que podemos hacernos a nosotros mismos y a nuestros descendientes, y sus posibles consecuencias. Este capítulo discute cambios en lo que sabemos y sus posibles consecuencias. Más conocimiento es, en conjunto, algo bueno, pero podría haber excepciones.

PADRES SABIOS

Los patrones de apareamiento humanos han variado mucho a lo largo del tiempo y del espacio, pero la monogamia a largo plazo está lejos de ser el más común. Este patrón (macho y hembra formando una pareja de apareamiento y siguiendo juntos durante un periodo extenso de tiempo) no es común en otras especies mamíferas. Lo es, de forma extraña, entre los pájaros, posiblemente porque su descendencia, como la nuestra, requiere un extenso cuidado de los padres. Hace mucho que se sabe que los cisnes y gansos, por ejemplo, se emparejan de por vida.

La investigación moderna ha mostrado que el comportamiento de la mayoría de variedades de pájaros emparejados es incluso más cercano a la de los humanos de lo que creíamos antes. Como con los humanos, la norma es la monogamia atenuada por el adulterio. Mientras que una pareja de apareamiento criará junta a sucesivas familias de pollos, una fracción significativa de esos pollos (las pruebas genéticas sugieren cifras del 10 al 40%) no son descendientes del macho de la pareja. Experimentos similares son más difíciles de preparar con los humanos, pero el trabajo que se ha realizado sugiere que un porcentaje significativo (las estimaciones van uno de cada cien a uno de cada tres) de los niños de las mujeres casadas que viven con sus maridos tienen a otro por padre. [96]

---

[96] Baker and Bellis, 1992, citado en Ridley, 1995: «En un bloque de pisos de Liverpool, encontraron mediante pruebas genéticas que menos de cuatro de cada cinco personas eran

Desde un punto de vista evolutivo, la lógica de la situación está clara. Los machos representan dos papeles diferentes en la reproducción humana (y aviaria). Contribuyen con genes para ayudar a producir hijos y recursos para ayudar a criarlos. La última contribución es costosa; la anterior, no. Un macho que puede fecundar a la pareja de otro macho obtiene éxito reproductivo (más copias de sus genes en la siguiente generación) a un precio insignificante. Así que no es sorprendente que los machos, sean hombres o gansos, inviertan un esfuerzo sustancial en intentar fecundar a hembras de las que no son pareja e intentando evitar que otros machos fecunden a sus parejas.

Una hembra leal obtiene ambos genes y apoyo de su pareja, intercambiando su contribución produciendo descendencia por la suya. Pero una hembra infiel puede salir más beneficiada. Se empareja con el que más provee para la prole y luego, cuando se le dé la oportunidad, dejará que la fecunde el macho de mayor calidad disponible, donde «calidad» se define por características observables cualesquiera que indiquen características hereditarias que pueda esperarse que resulten en éxito reproductivo para su descendencia: longitud de cola en las golondrinas, ingresos y estatus en los humanos. Como se supone que dijo Henry Kissinger, «el poder es el afrodisiaco definitivo»[97].

Esta estrategia funciona, para gansos y mujeres, por una característica curiosa de nuestra biología: la incapacidad de los machos para identificar con seguridad a su descendencia. Si no fuera el caso, si los machos estuvieran equipados con algún sistema intrínseco de identificación biométrica basada en el olor, apariencia o similar,

---

los hijos de los que se hacían llamar sus padres... Hicieron las mismas pruebas en el sur de Inglaterra y encontraron los mismos resultados». Numerosos estudios que realizan estimaciones de tasas de padres que cuidan a hijos ajenos entre humanos están resumidos en Baker y Bellis, 2007. Véase también www.meangenes.org, en particular http://www.meangenes.org/notes/notes.html#c8. Un estudio suizo, en contraste con el inglés, encuentra tasas de «paternidad mal atribuida» ligeramente por debajo del 1%. Una cifra similar surge del estudio genético islandés a gran escala. Un estudio exhaustivo de los escritos al respecto se encuentra en http://www.childsupportanalysis.co.uk/analysis and opinion/choices and behaviours/misattributed paternity.htm. A juzgar por eso, la tasa actual de paternidad mal atribuida probablemente varía, a lo largo de un amplio rango de sociedades humanas, entre el 1% hasta el 30%.

[97] Citado en *The New York Times*, 28 de octubre, 1973.

podrían negarse, y lo harían, a proporcionar apoyo para la descendencia de otros machos.[98]

Sabiduría tecnológica

Esta característica de la biología humana ha desaparecido. La prueba de paternidad ahora hace lo que la evolución no consiguió; proporciona a los hombres una forma fiable de determinar qué hijos son suyos. ¿Cuáles son las consecuencias probables? Comencé a pensar en esta cuestión en respuesta a una hipotética de un compañero: Supón que se volviera costumbre comprobar la paternidad de cada niño al nacer. ¿Qué sucedería?

La consecuencia obvia es que algunos hombres descubrirían que sus mujeres han sido infieles y algunos matrimonios se romperían como resultado. La que es un poco menos obvia es que las mujeres casadas con aventuras tendrían más cuidado con los anticonceptivos. La consecuencia todavía menos obvia (excepto para los economistas y los biólogos evolutivos) es que los hombres cuidarían más de sus hijos.

Desde el punto de vista del economista, la razón es que la gente valora el bienestar de su propia descendencia sobre el bienestar de la de otra gente. Desde el punto de vista del economista, la razón es que los seres humanos, como otras criaturas vivientes, han sido diseñados por la evolución para actuar de forma que maximicen su éxito reproductivo, y una forma de hacerlo es concentrar tus recursos limitados en tus propios hijos. De cualquiera de las maneras, la conclusión es la misma. La prueba de paternidad rutinaria significaría que los hombres sabían que sus hijos eran de verdad suyos y entonces estarían dispuestos a invertir más recursos en ellos. Invertirían menos en los niños que resultaron no ser suyos, pero habría menos de esos que antes, debido al deseo de las esposas de tener hijos a los que sus maridos ayudarán a

---

[98] Hay algunas pruebas de que los niños se parecen a los padres más que a las madres, lo que proporcionaría un sistema imperfecto de test de comprobación de paternidad intrínseco (Christenfeld y Hill, 1995). Pero véase también Bredart y French, 1995, que no consiguieron repetir el resultado, en http://www.u-bourgogne.fr/LEAD/people/french/father resemblance.pdf.

mantener. Y esos niños que sí tenían un padre que no era el marido de su madre podrían probarlo, y así tener al menos una esperanza de que se le mantenga.

Los lectores que cuestionan la suposición de que los padres son parciales a favor de sus propios hijos podrían querer echar un vistazo a las pruebas escritas. En una amplia variedad de culturas, se da por hecho que no se puede confiar en que los padrastros se preocupen de sus hijos adoptivos.[99] En una variedad de culturas hay pruebas de las estadísticas de maltratos y asesinatos de niños de que los libros no se equivocan: a juzgar por un estudio, es cuarenta veces más probable que los padrastros maten a niños que los padres reales.[100] Y, yendo más allá de nuestra especie, hay pruebas de que los pájaros machos ajustan la cantidad de cuidado parental que dan a los pollos atendiendo a la probabilidad de que los pollos no sean suyos.[101]

Hasta ahora he estado considerando una consecuencia directa de la combinación de una nueva tecnología y una nueva práctica social. La tecnología ya ha sucedido; la práctica, hasta ahora, no ha cambiado en respuesta a ella.

Sin embargo, la ley sí. Bajo la ley de Lord Mansfield, una doctrina del derecho consuetudinario que se remonta al siglo XVIII, a un hombre casado que vivía con su esposa se le prohibía legalmente cuestionar la legitimidad de su descendencia. Esto aparece en los estatutos modernos como la norma de que la madre de un niño es la mujer de cuyo cuerpo nace el niño y, si esa mujer estaba casada y vivía con su marido cuando se concibió el niño, se da por hecho concluyentemente que él es el padre.

Era una norma legal razonable siempre que no hubiera una forma práctica de demostrar la paternidad. La mayor parte del tiempo daba las respuestas correctas. Cuando no, por no general no había manera de hacerlo mejor y no tenía sentido consumir tiempo, esfuerzos e intentos de buena voluntad marital.

---

[99] Pinker, 2002.
[100] Buss, 2004, pp. 199–202. La figura que cita es de Daly y Wilson, 1988.
[101] Daly y Wilson, 1992, discute el comportamiento en los pájaros en relación a los celos sexuales masculinos; la página 294 proporciona el caso específico de una inversión parental variante. La prueba humana se encuentra en las páginas 306-308.

Ya no es una norma legal razonable y, cada vez más, ya no es la norma encarnada en las leyes modernas. En California, por ejemplo, un estado federado a cuyo derecho familiar volveremos al final de este capítulo, la ley actual concede que el supuesto se puede rebatir si hay pruebas científicas de que el marido no es el padre.

Si todos los padres son sabios...

Ya está bien del presente y el futuro inmediato. Una cuestión más interesante es el efecto a largo plazo de la tecnología. Una función de las instituciones matrimoniales de la mayoría de las sociedades humanas que conocemos, pasadas y presentes, es dar a los hombres una confianza razonable de paternidad estipulando que bajo la mayor parte de las circunstancias solo un hombre tenía acceso sexual a cada mujer. Con la prueba de paternidad moderna, ya no es necesario.

Esto plantea algunas posibilidades interesantes. Podríamos, en un extremo, tener una sociedad de promiscuidad ocasional: Samoa, al menos como la imagina Margaret Mead. Cuando nace un niño, el padre biológico, demostrado por la prueba de paternidad, tendría los derechos y responsabilidades paternas relevantes. Hay problemas con ese sistema. Es más fácil que dos progenitores críen a un niño conjuntamente si están viviendo juntos, y el hecho de que a dos personas les guste el sexo juntos es una prueba muy débil de que disfrutarán vivir juntos. Una alternativa más atractiva e interesante es alguna forma de matrimonio en grupo: tres o más personas viviendo juntos y criando juntos a los niños. Estos arreglos se han intentado en el pasado y no hay duda de que algunos existen ahora. La única forma que ha sido común (la poliginia, un marido con varias esposas) es la que no requiere prueba de paternidad para determinar la paternidad. La cuestión es si ahora se volverán más comunes otras formas.

Ella se reduce a una simple pregunta cuya respuesta no conozco: ¿están programados los celos sexuales masculinos? ¿Objetan los hombres a que otros duerman con sus parejas porque la evolución ha construido en ellos un fuerte deseo de exclusividad sexual o simplemente porque han elegido, o se les ha enseñado, esa estrategia

como forma de conseguir el objetivo (determinado evolutivamente) de no gastar sus recursos criando a los hijos de otro? Una débil prueba de la última explicación la proporcionó la observación de un antropólogo de que los hombres pasaban menos tiempo controlando a sus mujeres cuando estaban embarazadas, y, por tanto, no podían concebir.[102]

Una persona con la que he discutido este tema me informó de que él y gente que conocía no experimentaban celos sexuales; los lectores interesados en unirse a esta discusión deberían de ser capaces de encontrarle a él y algunos de sus amigos en el grupo de noticias de Usenet alt.polyamory, que significa lo que parece. Pero lo que estaba señalando podría haber sido solo la pequeña fracción de hombres que, porque tienen niveles anormalmente bajos de celos sexuales, están dispuestos a experimentar con patrones de apareamiento no convencionales.

Supón que los celos sexuales masculinos están programados. Todavía queda una posibilidad interesante: la madre profesional. Piensa en una mujer a la que le gustan los niños, es buena teniéndolos y criándolos y ella misma tiene características que gustarían a los hombres en la madre de sus hijos: saludable, inteligente, guapa. Júntala con hombres a los que les gustaría tener hijos pero que no han tenido éxito al encontrar una compañera dispuesta con la que les gustaría tenerlos. El hombre engendra al niño, sea por inseminación artificial o por medios más tradicionales. La mujer concibe y cría al niño. El hombre proporciona apoyo financiero y quizás una figura paternal.

Un problema con esto es que la madre ideal de tus hijos es preciosa, brillante y sana, y una mujer así podría ser capaz de encontrar una carrera más atractiva que ser una madre de alquiler. La tecnología reproductiva moderna tiene una solución. Ya hay un mercado próspero de óvulos humanos, en el que el precio depende de las características de la mujer que los donó; se venden buenos genes. La madre profesional podría ser solo el recipiente, concibiendo al mejor bebé construido mediante la combinación de tu esperma con el mejor óvulo que el dinero puede comprar.

¿Y si invertimos los papeles? Supón que es la madre la que desea construir su propio bebé, combinando su óvulo con los mejores genes

---

[102] Flinn, 1988, citado en Daly y Wilson, 1992, p. 302.

que pueda encontrar. Al tener su propio útero, no tiene que alquilar uno de otra persona, dando por hecho que está dispuesta a aceptar los costes de concebir ella misma al niño. También tiene una segunda ventaja. Los óvulos son relativamente escasos, ya que recogerlos de un ovario es un proceso desagradable e incómodo. El esperma es, para la mayor parte de propósitos prácticos, un bien gratuito. Dado un mercado bien desarrollado de esperma, etiquetado apropiadamente con las características del donante o quizás su mapa genético, la madre soltera que quiere tener el hijo debería de tener una gama de elección más amplia, a un precio más bajo, que el padre soltero que quiere tener el hijo.

Hay dos tendencias en la sociedad moderna de importancia creciente que podrían crear un patrón así. Una es los ingresos reales cada vez superiores; cuanto más rico sea, más fácil es que un padre o madre soltero críe al hijo. La otra es la mejora en nuestro conocimiento de la genética. Al final debería de ser posible que una pareja construya mejores bebés sobre todo a partir de sus propios genes, como se describe más adelante en este capítulo. Pero requiere mucho menos progreso (conocimiento genético, no de ingeniería genética) hacerlo usando los de otro.

¿Qué sucederá? Tendremos que esperar.[103]

EL PROBLEMA DE LOS PADRES

Si las nuevas tecnologías reproductivas van a generar nuevos problemas para la gente en el futuro o no, ya están produciendo problemas para el sistema legal y las instituciones sociales en que están insertadas.

El primero, y actualmente el mayor, es el problema de la paternidad. A las agencias del bienestar estatal y las madres solteras o divorciadas/viudas les gustaría encontrar un hombre al que se le pueda

---

103 Uno podría argumentar que ya ha pasado. Usando tecnología reproductiva antigua, muchas mujeres eligen concebir hijos a pesar de carecer de un padre dispuesto a ayudar a criarlos. La biología evolutiva sugiere que el padre se elige probablemente, al menos en parte, por características hereditarias que puede pasar a sus hijos. (Wright, 1994, Capítulo 3; Buss, 2004, Capítulo 6, especialmente pp. 175–186.)

hacer responsable de mantener a los niños de las madres. Si se puede identificar a su padre genético, es el candidato obvio. ¿Pero y si no?

La visión de algunos países es que el hombre que era el compañero de la madre debería ser responsable sea o no el padre real: un retroceso a la norma de Lord Mansfield, extendida para cubrir a las parejas no casadas. Podía funcionar antes de la prueba de paternidad moderna porque el Estado podía argumentar que era probable el hombre con el que ella había estado viviendo, quizás con el que estaba casada, fuera el padre genético de sus hijos incluso si lo negaba. Ese argumento ya no funciona ahora que puede probar que no lo es.

El argumento obvio para la otra parte es que un hombre al que se le han puesto los cuernos ya es una víctima de la traición de la madre; hacerle responsable de mantener al hijo de otro solo añade daño al insulto. El contraargumento es que incluso si la madre tiene la culpa, su hijo no, y requiere que alguien lo mantenga. El argumento se vuelve más convincente si el hombre ha actuado como padre para el hijo durante suficiente tiempo para establecer un lazo emocional entre los dos.

Una posibilidad para un poco más a la larga es una base de datos genética que podría usarse para identificar al padre genético y hacerle responsable, retornando a la idea de la prueba de paternidad en el nacimiento. Una alternativa menos ambiciosa es exigir a la madre que identifique al padre o posibles padres y que el Estado lo obligue a permitir que se realice la prueba. Pero si la madre no está dispuesta o no es capaz de identificar al padre, volvemos al problema de quién, más que el Estado, puede hacerse responsable.

La prueba de paternidad también podría crear problemas para los hombres que, bajo la ley actual, no son responsables de mantener a niños que, genéticamente hablando, son realmente suyos. En muchos estados federados, si una mujer concibe mediante inseminación artificial usando el esperma de un banco de esperma, no puede pedir manutención al donante. Antes de la prueba de paternidad, esa norma legal podía ejecutarse simplemente no guardando los registros relevantes. Hoy los registros que establecen paternidad están marcados en cada célula del padre y el hijo. Si la ley y la costumbre cambian, como han cambiado en el pasado hacia la dirección de hacer más fácil

que los hijos adoptivos encuentren a sus padres, incluyendo a los que no quieren ser localizados, algunos hombres podrían recibir una sorpresa.

Dos, cuatro, muchos

La prueba de paternidad puede establecer el factor de la paternidad. Pero no nos dice qué significa paternidad, o maternidad. Podemos determinar mejor que en el pasado quién tiene qué relación con un niño. Pero también podemos producir relaciones más complicadas, haciendo más difícil que encaje la nueva realidad con la antigua ley.

Con la tecnología y práctica actuales, el término «madre» tiene al menos tres significados diferentes. Uno es la que quiere ser madre: la mujer que tiene la intención de representar el papel social de la madre cuando se han arreglado las preparaciones para producir al hijo. Una es la madre de útero: la madre en cuyo útero crece el feto. Una tercera es la madre del óvulo: la mujer que proporcionó el óvulo. Una vez comencemos a clonar humanos, una cuarta categoría será la madre mitocondrial: la madre que proporciona el óvulo cuyo núcleo se reemplaza por el núcleo de una célula del clon donante, manteniendo el ADN extranuclear de la mujer.

Los padres todavía vienen en dos modalidades. El que quiere ser padre es el hombre que tiene la intención de representar el papel social de padre; el padre biológico es el hombre que proporcionó el esperma. El único cambio asociado con la tecnología más nueva es que es más común de lo que solía ser que el que desea ser padre sepa que no es el padre biológico.[104] Con tres o cuatro variedades de madre y dos de padre, la definición de «padres» se vuelve seriamente ambigua.

Ese problema se mencionó en el capítulo 2, donde describía el caso (real, California) del niño con cinco padres. Los cinco eran gente distinta, y los que tenían el deseo de ejercer de padres, John y Luanne, se separaron un mes antes de que naciera el bebé. El tribunal decidió

---

[104] Casanova, en sus memorias, describe una aventura con una mujer casada cuyo marido era impotente, llevada a cabo con el apoyo del marido para proporcionarle descendencia legal. (Casanova, 1971, volumen XI, Capítulo 10.)

que ellos eran los que contaban. Aunque ninguno tenía ninguna conexión biológica con el niño, Luanne acabó con el Bebé, John fue responsable de mantenerlo.

La misma solución legal podría usarse para resolver los problemas de la paternidad planteados por la clonación. El clon humano obtiene todo su ADN nuclear de un donante. Genéticamente hablando, uno podría describir a ese donante como ambos padres. Si hiciéramos las pruebas genéticas usuales, mostrarían que el clon es hijo de los padres del donante. Surgen más complicaciones del ADN extranuclear, que viene de la mujer que donó el óvulo usado en el procedimiento y podría o podría no ser el donante del ADN nuclear. Y, puesto que se pueden obtener células de un donante sin su consentimiento, tenemos la posibilidad de que una mujer pueda concebir al clon de un hombre rico e importante y luego demandarlo por manutención del niño en una escala apropiada a su renta. El caso más cercano del mundo real que conozco bajo la tecnología actual es uno en el que aparentemente una mujer se quedó embarazada con esperma obtenido fraudulentamente y consiguió establecer una demanda de manutención del niño contra el padre.

La definición establecida por el tribunal de California (que la paternidad venga determinada por la intención de ser padre) proporciona una sencilla norma para cubrir casi todas las circunstancias, sea cual sea la tecnología reproductiva; para que el niño exista, al menos una persona tuvo que desearlo, o al menos elegir realizar acciones que pudieran llevar a ello, y esa persona cuenta como padre o madre. Todavía deja algunos problemas.

La reproducción convencional involucra a un hombre y una mujer. Una vez se puede subcontratar la biología, la intención de reproducirse podría involucrar a un hombre y una mujer, dos hombres, dos mujeres, una asociación de cuatro de cada, o una corporación (digamos Microsoft, buscando criar a un sucesor para Bill Gates). Solo el patrón convencional se encuadra dentro de las normas legales diseñadas para ese patrón. Una vez aceptamos la paternidad deseada, la ley debe restringir quién puede ser un padre en intención (exigir, por ejemplo, que antes de que pueda tener lugar cualquier forma de reproducción asistida, un hombre y una mujer (en la versión más conservadora)

deban identificarse como que tienen la intención de ser padres, o especificar obligaciones y derechos de paternidad lo bastante amplios para que cualquiera de los acuerdos permitidos puedan encajar en ellos.

Hace mucho tiempo que ha existido un problema similar, y se ha tratado con la ley durante mucho tiempo: la empresa. Para muchos fines, tratamos a las empresas como si fueran personas; hacemos contratos con ellos, les vendemos cosas, compramos cosas suyas, los denunciamos por daños y perjuicios. Para hacerlo, hemos tenido que proyectar los derechos y responsabilidades de un solo individuo en organizaciones de una amplia variedad de tipos. Tenemos que decidir lo que para una firma significa acceder a algo, ser responsable de hacer algo, tener responsabilidad de algo, qué actos reales de seres humanos vivientes, que respiran cuentan como actos de una persona ficticia en cuyo nombre están actuando. Definir la paternidad, en el mundo que está creando la tecnología reproductiva moderna, presenta un problema casi análogo.

LA GENTE CONSIDERADA COMO PROPIEDAD INTELECTUAL

Cuando Monsanto, la compañía de biotecnología agrícola líder, creó una soja transgénica, la patenta; si otra gente realiza copias sin permiso usando el cultivo de este año para la semilla del siguiente sin pagar a Monsanto por el derecho a hacerlo, están infringiendo la patente de Monsanto. Algunos de los problemas planteados por esa situación los discutiremos en el próximo capítulo.

¿Y si Monsanto aplica sus nuevas tecnologías no a la soja, sino a la gente, al producir una versión mejorada con algunos genes nuevos, trasplantados de otra especie o creados en el laboratorio? Frente a esto, parecería que se aplica la misma ley. Ahora tienes seres humanos que en parte pertenecen a otro; uno o más de los genes de cada célula son propiedad intelectual de Monsanto.

Las criaturas vivas, incluyendo los humanos, están creando continuamente nuevas células para reemplazar a las viejas, así que parece como si el bebé patentado infringiera la patente con cada respiración. La solución obvia es que el contrato mediante el cual se

produce el bebé incluya una licencia de por vida para usar la patente dentro del cuerpo de ese niño, así como el contrato mediante el que el agricultor compra soja creada mediante ingeniería genética incluye el derecho a que las plantas resultantes reproduzcan sus genes patentados en el proceso de crecimiento.

¿Y realizar copias que acaben fuera del cuerpo del niño? Si soy el niño, ¿necesito el permiso de Monsanto para reproducirme? ¿Para realizar cualquier actividad que podría llevar a la reproducción? Quizás la licencia original debería incluir algunos términos adicionales, con precios fijados de antemano.

Considerando que la actitud que adopta nuestro sistema legal frente a la propiedad privada de humanos por parte de otro que no sea ese mismo humano, dudo de que Monsanto pueda llegar muy lejos ejecutando sus derechos de propiedad intelectual en este contexto nuevo, pero nunca se sabe. Es improbable que surja este asunto. Los seres humanos maduran lentamente. Para cuando me haya interesado seriamente en infringir la patente que hay sobre mí, probablemente habrá expirado.

La soja, por otra parte, no tiene derechos individuales a la autoposesión y sus generaciones solo duran un año. Para la soja, el asunto de los derechos de propiedad intelectual en las cosas que viven y reproducen es real, actualmente encarada por tribunales de una variedad de países.

¿ES LA IGNORANCIA UNA DICHA?

… y *las* mil *conmociones* naturales / de las que esa carne es heredera…
Hamlet

De todas las enfermedades de las que la carne humana es heredera, algunas se deben completamente a tener los genes erróneos (la anemia falciforme, por ejemplo). Muchas otras, como una enfermedad coronaria y el alzheimer[105], parecen tener un componente genético sustancial. A medida que mejoran el conocimiento y la tecnología, cada

[105] Ridley, 1999, pp. 258–264.

vez seremos capaces de identificar a individuos que tengan o no los genes que les hace más probable morir jóvenes de un ataque al corazón, convertirse en alcohólicos o sufrir otras consecuencias indeseables. Ya es posible hacer un mapa completo de los genes de un individuo por menos de un millón de dólares y se predice que el coste bajará de los mil dólares en un futuro no muy lejano. Combínalo con un conocimiento adecuado que conecte los genes con las consecuencias y se vuelve posible saber mucho sobre tus perspectivas de futuro.

Alguien que sabe está predispuesto genéticamente a enfermedades coronarias tiene buenas razones para tomar mayores precauciones contra ello: ejercicio, dieta, pruebas y similares. Que mi abuelo muriera de un ataque al corazón y a mi padre se le haya realizado un baipás son buenas razones para que tome medicación para bajar el colesterol e intentar hacer ejercicio regularmente. Pero habría tenido mejores motivos para esa decisión si supiera si llevo o no los genes que causaron esos problemas a mi padre y abuelo; mientras que todavía no tenemos información completa sobre la genética de las enfermedades coronarias, sí sabemos que llevar ciertas variantes de ciertos genes incrementa sustancialmente las posibilidades de morir de un ataque al corazón. Y alguien que supiera que es, por razones genéticas, particularmente vulnerable al alcoholismo podría elegir evitar el problema no tomando nunca su primera bebida.

¿Y si tengo un problema genético para el que no hay solución, como el de un gen que tenga como resultado un envejecimiento anormalmente rápido? Saber que lo tengo al menos me permite realizar una mejor planificación de mi vida, como tener hijos pronto o no tenerlos en absoluto. Pero el conocimiento no es algo inevitablemente deseable. Si llevo una sentencia de muerte en mis generes, podría preferir no saberlo. A veces la ignorancia es una dicha, al menos por un tiempo.

Hasta ahora he estado considerando el efecto del conocimiento de mis genes. De lo que otra gente sabe de ellos podrían surgir problemas algo diferentes. Piensa en una compañía de seguros que ofrece seguros contra una enfermedad que es completamente genética en un futuro en que la prueba genética fiable está disponible al instante. Una vez lo esté, el riesgo de enfermedad deja de estar asegurada por una empresa. Solo la gente que sabe que tienen los genes relevantes comprarán el

seguro, y los vendedores, sabiéndolo, le pondrán un precio en consecuencia.

¿Y la situación más realista en que un problema es en parte genético? El coste esperado de asegurarme contra el problema depende entonces de qué genes tengo. Si se permite que las compañías de seguros insistan en realizar pruebas a los clientes antes de venderles un seguro, tanto los que tienen malos genes como los que no serán capaces de comprar un seguro, pero con precios diferentes. La parte del riesgo por tener genes malos ya no se puede asegurar, lo que deja el seguro solo para riesgo residual, la incertidumbre de la enfermedad de alguien con una propensión genética conocida. En el caso más realista en que contra lo que te estás asegurando no es un riesgo particular, sino el efecto combinado de muchos riesgos (el caso del seguro de vida o salud), el resultado es el mismo. Tu esperanza de vida depende en parte de tu estructura genética y en parte de otras cosas. La incertidumbre por lo primero no se puede cubrir con un seguro; la incertidumbre por lo último sí.

La solución que algunos han recomendado es ilegalizar que las compañías de seguros exijan pruebas. Los individuales todavía pueden someterse a las pruebas, y lo harán. Si descubro que soy extraordinariamente afortunado en cuanto a genética, también sé que el seguro de vida y de salud, con un precio basado en el supuesto de que soy normal, son malas apuestas. Si, por el contrario, sé que es probable que caiga muerto a los cuarenta, entonces tener muchos seguros de vida, siempre que espere tener supervivientes que me importen, es obviamente un buen negocio.

Este efecto se conoce en los escritos de seguros como *selección adversa*; ocurre cuando una parte de una transacción tiene información sobre la calidad de lo que se está vendiendo que la otra parte no tiene ni puede obtener. Un ejemplo estándar es el mercado de coches usados. Los compradores ignorantes pagan el mismo precio para los coches buenos (profiteroles) que para los coches malos (limones), lo que hace que la venta de tu coche sea un buen negocio si tienes un limón y un negocio malo si tienes un profiterol. Los limones se venden y los profiteroles, en su mayoría, no. Los compradores, anticipándolo, hacen su oferta con el supuesto de que si se acepta la oferta, el coche es

probablemente un limón, y a precios de limón, se venden pocos profiteroles.

La lógica es aquí la misma. Imagina que las compañías de seguros comienzan cobrando una tasa que simplemente cubre los costes en el caso de un cliente medio. El seguro es un negocio mucho mejor para los clientes con genes que hacen probable que cobren que para los clientes con genes que hacen improbable que cobren, así que los compradores de un seguro incluyen un número superior a la media de malos riesgos. Las compañías de seguros lo descubren y suben sus tasas, expulsando más riesgos buenos. En el caso límite, cuando se han expulsado todos los riesgos buenos, el resultado es todavía peor de lo que sería si las compañías hicieran pruebas. Nadie puede tener seguro contra el riesgo genético, porque la decisión de comprar el seguro dice al vendedor que el comprador sabe que tiene malos genes. Aquellos que tienen malos genes todavía pueden coger un seguro contra el riesgo por otras causas; aquellos que tienen buenos genes no.

Una solución sería hacer posible de algún modo demostrar que nunca se te ha hecho una prueba. Ahora la gente puede obtener primero un seguro, y luego pedir cita para la prueba y modificar sus planes de vida en consecuencia. Por desgracia, un sistema así proporciona un gran incentivo para engañar, que se te haga la prueba en el mercado negro o en un país extranjero para no dejar ningún registro y entonces decidir qué seguro comprar tras ver los resultados.

Una solución alternativa sería que los padres compraran los seguros de sus hijos antes de que se los conciba. El precio podría depender todavía de los genes de los padres, pero no puede depender de los de los hijos, ya que esa es una información que nadie tiene. No, al menos, hasta que hayamos pasado por todos los desarrollos descritos en el anterior capítulo, un punto en el que ya no quedarán genes malos de los que preocuparse.

Por supuesto, las compañías de seguros no son la única gente que podría estar interesada en tus genes. Ahora hay alguna prueba de que una tendencia hacia la fidelidad (o infidelidad) sexual es en parte genética. Exigir una prueba genética de tu prometido justo antes del matrimonio parece un poco grosero, pero quizás, en un futuro en que las tecnologías relevantes estén bien desarrolladas y completamente

explotadas, las preguntas se plantearán (en el casamentero en línea) antes de la primera cita.

GÉNERO AMBIGUO

Estamos acostumbrados a dar por hecho que cada uno de nosotros es hombre o mujer. Durante mucho tiempo era una aproximación bastante buena.[106] Pero no por mucho tiempo. Una razón es el conocimiento proporcionado por la biología moderna. Casi todos los hombres tienen un cromosoma X y uno Y y un cuerpo masculino; casi todas las mujeres tienen dos cromosomas X y un cuerpo femenino. Pero hay excepciones. Algunos humanos tienen XY pero tienen cuerpos femeninos: genéticamente hombres pero morfológicamente mujeres. Algunos son lo contrario: XX con cuerpos masculinos. Y algunos hombres son genéticamente XYY, con cuerpos masculinos y una pequeña tendencia hacia personalidades agresivas, o XXY, o...

Hasta ahora hemos estado tratando de genética y morfología, ambas bastante poco ambiguas incluso si las combinaciones son más salvajes de lo que pensábamos. La situación se vuelve más confusa si introduces la psicología. Alguna gente que es genética y morfológicamente hombre afirma que es psicológicamente mujer, que piensa en sí mismo como mujer. Otros tienen el patrón contrario. Hay alguna prueba de que esto es más que una alucinación, que de alguna forma que aún no entendemos claramente, esa gente tiene cerebros diseñados para el género erróneo. Las técnicas quirúrgicas modernas hacen posible corregir al menos en parte el error: que a alguien que se identifica con una mujer en el cuerpo de un hombre al menos se le ponga en una copia razonable del cuerpo de una mujer, aunque estéril. Lo mismo al revés.

Todo esto plantea problemas interesantes para los individuos y la ley. ¿Voy a pensar en Deirdre, un compañero profesional que solía ser Donald, como una mujer, un hombre cambiado mediante cirugía para que parezca una mujer, o algo que no es hombre o mujer? Si hubiera discutido estos asuntos con Donald cuando poseía, según su visión, el

---

[106] Las únicas excepciones obvias eran las hermafroditas y eunucos.

cuerpo de un hombre pero la mente de una mujer (no lo hice), ¿cómo debería haber pensado en la persona con la que estaba discutiéndolas? Si Deirdre se casa con un hombre rico y luego muere intestado, ¿pueden sus descendientes cuestionar con éxito su exigencia de recibir una parte de su propiedad basándose en que ella era un él, y por tanto no podía contraer un matrimonio legal con un hombre? Este caso particular (con un transexual diferente) se llevó a los tribunales recientemente en Kansas. La esposa perdió.

Va a ser un siglo interesante.

QUINCE

COMO DIOSES EN EL JARDÍN

El día en que comáis de él serán abiertos vuestros ojos y seréis como dioses...

Génesis 3:5

El capítulo anterior trataba de una pequeña parte de la biotecnología: su aplicación a los humanos. Este capítulo trata de las aplicaciones de la misma tecnología a otras cosas vivientes.

CULTIVOS DISEÑADOS

La biotecnología agrícola es una de las formas más antiguas de alta tecnología, que se remonta a al menos ocho mil años. Fue entonces, según estimaciones actuales, cuando comenzó el programa de cultivo que terminó por producir el maíz, posiblemente a partir de teosinte, una planta que la mayoría de nosotros describiríamos como una mala hierba. Programas similares de cultivo selectivo son responsables de crear todas nuestras plantas principales que utilizamos como alimento.

No solo es una tecnología antigua la creación de cadenas genéticamente superiores mediante mutación aleatoria y cultivo o cría selectiva, también lo es la clonación. Desde hace mucho tiempo se ha sabido que los árboles frutales no se cultivan con fidelidad a la semilla. Para probarlo por ti mismo, quita las semillas de una manzana golden, plántalas, espera diez o veinte años y mira lo que obtienes. Las posibilidades de que no sea una golden ni moderadamente buena son tan abrumadoramente altas que no será nada que quieras comer.

La solución es el injerto. Una vez tenga el pequeño manzano sus raíces bien crecidas, reemplaza la sección de arriba del tronco por una pieza de una rama cortada de un manzano golden. Si lo haces bien, la nueva madera crecerá sobre la vieja; todo lo que se encuentre sobre el injerto será golden, genéticamente hablando, incluidas las manzanas. Acabas

de producir un clon, un organismo (al menos la mayor parte de un organismo) que es genéticamente idéntico a otro. Como Dolly, la oveja clonada, tu árbol clonado se creó usando células de un organismo maduro.

Para ser incluso más extravagante, deja que crezca el árbol hasta que tenga unas pocas ramitas y entonces reemplaza el final de una rama por un trozo de madera de un manzano golden, una segunda por un trozo de un manzano swaar (de manzana fea pero deliciosa) y una tercera por un trocito de una manzana lady (diminuta, bonita, sabrosa). Ahora tienes todo ese catálogo, una manzana tres en una. También acabas de usar, en tu propio jardín, una forma de biotecnología que se ha conocido al menos desde los tiempos de los romanos y es en gran parte responsable de la calidad de la fruta, uvas y vino de los varios últimos miles de años.

Nuevo bajo el sol

La biotécnica agrícola moderna añade al menos dos nuevos elementos a las antiguas tecnologías de injerto y cultivo selectivo. Una nos da la habilidad de hacer mejor lo que hemos estado haciendo. La otra nos proporciona la habilidad de hacer algo casi completamente nuevo.

La forma tradicional de cultivar una manzana mejor es crear un número muy grande de semillas, plantarlas todas ellas, dejarlas crecer y ver cómo salen. Si, con mucha suerte, una resulta ser de una variedad superior, a partir de ahí puede propagarse mediante los injertos. Con el suficiente conocimiento experto, el cultivo de plantas puede mejorar un poco las probabilidades eligiendo a los padres correctos, eligiendo un par de árboles que tengamos razones para esperar que puedan producir una descendencia superior, polinizando uno con polen del otro y usando las semillas resultantes. Pero todavía es en gran parte una apuesta.

A medida que mejoren nuestro conocimiento de la genética y nuestra capacidad para manipular genes, podríamos ser capaces de actuar mejor. Si descubrimos qué secuencias particulares de genes están relacionadas con rasgos deseables en particular, podemos mezclarlas y

unirlas para producir árboles (o vides, o plantas para dar tomates) con los rasgos que queramos. Estaremos haciendo lo mismo que podríamos hacer hecho con las viejas tecnologías, pero en mucho menos de ocho mil años.

Una posibilidad más curiosa e interesante es añadir a una especie genes de otra, produciendo plantas transgénicas. Un ejemplo famoso (y comercialmente importante) utiliza *Bacillus thuringiensis*, o Bt, una bacteria que produce proteínas venenosas para algunos insectos pero no para humanos u otros animales. Se han producido variedades de plantas añadiéndoles los genes de la bacteria Bt responsable de fabricar esas proteínas. Las plantas de este tipo producen, en efecto, su propio insecticida. Otras plantas transgénicas están diseñadas para ser resistentes a herbicidas usados de forma global, lo que permite a un agricultor matar malas hierbas sin herir la cosecha.

Se puede utilizar también la misma tecnología para alterar la cosecha final, con lo que se producen cacahuetes o tomates con un tiempo de conservación más largo, o aceite de girasol que combine tiempo de conservación largo con bajos niveles de grasas saturadas y trans. También es posible insertar genes en una planta (o animal) que obtengan como resultado la producción de algo no relacionado con su cultivo normal. Los ejemplos incluyen bacterias modificadas para producir insulina, una vaca cuya leche contenga proteínas de leche humana y una oveja cuya leche contenga un factor coagulante que falta en la sangre de los hemofílicos.

Las plantas resistentes a los insectos nos permiten plantar cultivos a un coste menor y con mucho menos uso de insecticidas. Otras aplicaciones de la tecnología incrementan el rendimiento de los cultivos, reducen costes, mejoran la calidad y proporcionan formas de bajo coste de producir valiosos fármacos, incluyendo algunos que no se pueden, al menos hasta ahora, producir de cualquier otra forma. Aun así, se ha atacado fieramente a la tecnología; en algunas partes del mundo, sobre todo en Europa, se restringen severamente las aplicaciones agrícolas. ¿Por qué?

¿Un nido de serpientes?

Abu Hurairah (que Alá esté satisfecho con él) contó que el Profeta (que la paz y las bendiciones de Alá caigan sobre él) dijo: «Alá, que ensalzado sea, dice: "¿Quién hace más mal que el que intenta crear algo como Mi creación? Que cree un grano de trigo o de maíz»

Contado por al-Bukhari, *Fath al-Baari*, 10/385

Una razón es obvia: la hostilidad contra cualquier novedad, combinada con una visión romántica de la naturaleza. A mucha gente le gusta la idea de los «alimentos naturales», aunque prácticamente nada de lo que comemos sea natural en el sentido de no haber sido alterado sustancialmente por la actividad humana. Y usamos el término «químico» peyorativamente, a pesar del hecho de que todo lo que comemos y todo de lo que estamos hechos es una combinación de química. Se muestra la misma actitud en la descripción de los productos de la biotecnología agrícola como «Frankenfoods». La tradición musulmana citada más arriba refleja una versión religiosa de esta visión: crear cosas vivientes es asunto de Dios, no nuestro.[107]

Esta actitud es hoy de una importancia considerable; durante los próximos diez o veinte años, esto podría tener como resultado en los consumidores europeos la obtención de alimentos de menor calidad a precios más altos de los que obtendrían si no criticaran los alimentos genéticamente alterados. Una razón por la que podría suceder es que los agricultores europeos están subvencionados por los Gobiernos y protegidos de la competición extranjera por barreras comerciales. A cuantos más consumidores europeos se pueda persuadir de que los alimentos extranjeros son maléficos y peligrosos, más fácil es que los agricultores europeos vendan lo que cultivan.

---

[107] Un asunto que es particularmente probable que cause dichas preocupaciones es la introducción de genes humanos en otras especies, humanas o animales, para producir lo que se podría describir como quimeras. Véase http://www.futurepundit.com/archives/003647.html para una discusión reciente sobre el tema, y véase http://www.daviddfriedman.com/Academic/Course Pages/21st century issues/legalissues 21 2000 pprs web/21st c papers 2000/green monsanjo.htm para un entretenido trabajo de un estudiante al respecto, escrito para el seminario que produjo este libro.

Mientras que la hostilidad irracional podría ser importante a corto plazo, es probable que vaya a menos a la larga. Hay amplias partes del mundo en que incrementar la producción agrícola signifique que menos gente esté hambrienta, lo que hace los asuntos simbólicos de natural o antinatural irrelevantes en comparación. Y con el tiempo, lo nuevo se convierte en viejo. Los anticonceptivos se veían antinaturales, malvados, sucios y pecaminosos cien años atrás. La fecundación *in vitro* se recibió al principio con una actitud de sospecha. Ahora ambas se aceptan globalmente. Desde un punto de vista que va más allá de la próxima década la cuestión interesante es si hay algún problema real asociado a este tipo de tecnología. La respuesta es casi seguro que sí. Hay tecnologías poderosas, y las cosas poderosas pueden hacer daño tanto como bien. Piensa en un ejemplo simple.

Nuestras plantas alimenticias más comunes se cultivaron a partir de plantas silvestres preexistentes. Muchas de las últimas todavía están por ahí y, hasta cierto punto, pueden cruzarse con sus descendientes «domesticadas». Esto significa que los rasgos genéticos introducidos en las plantas de cultivo podrían, como polen soplado por el viento, ir a parar a plantas silvestres con parentesco. La resistencia a los herbicidas es una característica útil en una planta de cultivo. Es una molestia considerable en una mala hierba. Lo serio que sea este tipo de problema depende de si las plantas de cultivo transgénicamente mejoradas se cultivan cerca de las silvestres con parentesco, si la modificación es beneficiosa para las malas hierbas y si la modificación hace a las malas hierbas más problemáticas para los humanos.

Piensa en un tomate transgénico diseñado para tener un sabor mejor o un tiempo de conservación mayor. Incluso si hay plantas silvestres emparentadas, esas características no tienen una utilidad particular para ellas, así que las plantas silvestres con esas características no tendrían ventaja sobre las que no las tienen y no serían un problema para los agricultores.

No sucede lo mismo con la resistencia a los herbicidas. Supón que la remolacha silvestre crece cerca de los campos que contienen remolacha azucarera transgénicamente modificada para hacerla resistente a los herbicidas. Las remolachas silvestres que han tenido la buena suerte de

adquirir los genes de la resistencia serán más exitosas en esa localización que las que no, y más incordio.

¿Podemos competir con la Madre Naturaleza?

Volviendo atrás un momento, merece la pena mirar el argumento general por el que estos problemas no pueden existir y ver por qué a veces está mal. El argumento empieza con la observación de que las plantas existentes, incluidas las malas hierbas, han sido «diseñadas» por la evolución de Darwin para su propio éxito reproductivo. Nuestra biotecnología actual es un sistema de diseño mucho más primitivo que la evolución: por eso producimos nuevos cultivos no diseñando la planta entera desde la raíz, sino añadiendo modificaciones menores a las plantas proporcionadas por la naturaleza. Por tanto, uno podría esperar que si una característica genética que pudiéramos darle a una mala hierba fuera útil, la planta ya la tendría.

Hay dos errores en ese argumento. El primero es que la evolución es lenta. Las malas hierbas están adaptadas a su ambiente, pero ese ambiente ha incluido solo recientemente a agricultores echándoles herbicida. Así que no se han adaptado, o al menos aún no se han adaptado muy bien, a resistir esos herbicidas. Si creamos deliberadamente plantas de cultivo resistentes a herbicidas específicos y la resistencia se extiende a las malas hierbas emparentadas, proporcionamos un atajo evolutivo, una forma de generar malas hierbas con resistencia sustancialmente más rápido de lo que haría la naturaleza.

El segundo error en la argumentación es más complicado. La evolución no funciona diseñando nuevos organismos de cero, sino mediante una serie de pequeños cambios. Cuantos más cambios simultáneos se necesiten para hacer funcionar una característica, menos probable es que aparezca. Las estructuras complicadas (el ejemplo estándar es el ojo) se producen mediante una larga serie de cambios, cada uno de los cuales proporciona al organismo al menos una pequeña ganancia en éxito reproductivo. Es improbable que las características que no se pueden producir así se produzcan en absoluto.

La ingeniería genética también funciona mediante pequeños cambios: introducir un gen de una bacteria en una variedad de maíz, por ejemplo. Pero la gama disponible de pequeños cambios es distinta. Podría haber algunos cambios en un organismo que resulten en un éxito reproductivo mayor, y por tanto se habría seleccionado mediante evolución, que pueden producirse mediante ingeniería genética, pero es improbable que surjan de forma natural. La introducción de genes que codifican una proteína particular letal para plagas de insectos particulares, genes prestados de una criatura viva sin relación alguna, es un ejemplo. Este es un tema al que volveremos en un capítulo posterior, cuando pensemos en los intentos todavía más ambiciosos de la nanotecnología por competir contra el diseño natural.[108]

La posibilidad de que los genes producto de la ingeniería se extiendan por poblaciones silvestres y produzcan malas hierbas mejoradas es un ejemplo de una clase de asuntos planteados por la tecnología genética. Otros incluyen la posibilidad de efectos ecológicos indirectos: malas hierbas mejoradas, o plantas de cultivo que se vuelvan silvestres, que compitan con otras plantas y así alteren todo el sistema interrelacionado. También incluyen efectos imprevistos, como que las plantas de cultivo diseñadas para ser letales contra plagas de insectos también se vuelvan letales contra especies de insectos no dañinos, incluso beneficiales. Comienzo con el caso de las malas hierbas transgénicas porque pienso que es el caso más claro de un problema que es probable que suceda, aunque no sea probable que tenga consecuencias catastróficas. Si, después de todo, las remolachas silvestres se vuelven resistentes al herbicida favorito de los agricultores, siempre pueden cambiar al segundo que más les guste, lo que los sitúa de nuevo al principio, con un herbicida al que ni las malas hierbas ni el cultivo son especialmente resistentes.

Soy más escéptico sobre los otros ejemplos, sobre todo porque lo soy respecto a la idea de que la naturaleza se encuentre en un equilibrio

---

[108] A veces se sugiere que una diferencia crucial entre la ingeniería genética y la evolución es que la primera permite alteraciones transgénicas (la inserción del ADN de una especie de genes desde otra). Sin embargo, hay alguna prueba de que los desarrollos evolutivos importantes, incluyendo la fotosíntesis en organismos multicelulares, son debidos a alteraciones transgénicas naturales, posiblemente «construidas» por los virus. Para una discusión de esto, véase Knoll, 2004.

delicado susceptible a producir una catástrofe si se altera. La extinción de viejas especies y la evolución de las nuevas es un proceso que lleva sucediendo mucho tiempo. Pero mientras que soy escéptico respecto a ejemplos particulares, creo que ilustran un problema potencial real que surge del cambio tecnológico, probablemente el problema más serio.

El problema surge cuando las acciones tomadas por una persona tienen sustanciales efectos dispersos sobre muchas otras. La razón por la que es un problema es que no tenemos un conjunto de instituciones adecuado para vérnoslas con estos efectos. Los mercados, los derechos de propiedad y el comercio proporcionan unas herramientas muy poderosas para coordinar las actividades de una multitud de actores individuales. Pero su funcionamiento exige alguna forma de definir los derechos de propiedad de forma que la mayor parte del efecto de mis acciones sea concebido por mí, mi propiedad y un conjunto de otras personas razonablemente pequeño e identificable.

Si no hay forma de definir los derechos de propiedad que cumplan ese requisito, tenemos un problema. Las instituciones alternativas (tribunales, derecho de responsabilidad civil, regulación gubernamental, negociaciones intergubernamentales y similares) que usamos para lidiar con ese problema funcionan de forma muy pobre. Cuanto más dispersos estén los efectos, peor funcionan. Si los cambios tecnológicos que tienen como resultado crear acciones con efectos dispersos representan un papel mucho mayor en nuestras vidas; si, por ejemplo, la ingeniería genética significa que mis genes tocados por la ingeniería acabarán mostrándose en las malas hierbas de tu jardín a más de mil kilómetros de distancia, tenemos un problema para el que ninguna institución conocida proporciona una solución razonablemente buena. Es un asunto al que volveremos en capítulos posteriores.

Protección tecnológica para la biotecnología

En el capítulo 8 consideramos el problema de proteger la propiedad intelectual en formato digital en un mundo en que reproducirla es barato y sencillo. El mismo problema surge con la biotecnología

agrícola, donde el producto viene completo con el mismo que la copia. Una solución posible es usar la ley de propiedad intelectual para evitar que los agricultores compren el cultivo genéticamente modificado una vez y produzcan sus propias semillas de ahí en adelante. Esto debería de funcionar mejor para los cultivos que para los programas informáticos, ya que la infracción, si tiene lugar, sucede a gran escala en grandes espacios abiertos.

Una solución diferente es la protección tecnológica, alguna forma de vender el objeto que contenga la propiedad intelectual mientras que evita que el comprador copie lo que contiene. En una versión más antigua de la biotecnología agrícola, las variedades de semillas híbridas, esto sucedía automáticamente. Un agricultor compraba semillas híbridas, las plantaba, cosechaba el cultivo. Si luego volvía a plantar lo que había cosechado, el resultado, gracias a la magia de la reproducción sexual, sería un cultivo con características variantes, que refleja el proceso aleatorio que determina qué genes de cada padre acaban en qué semilla. Un cultivo así era más difícil de trabajar que la cosecha uniforme de las semillas híbridas adquiridas, así que la compañía de semillas podía vender más semillas cada año.

Esto no funciona con esas especies transgénicas que no dependen de la hibridación controlada, especies que crecen lo suficientemente fieles a la semilla para los propósitos de los agricultores. Para enfrentarse a ese problema, los investigadores desarrollaron y patentaron una forma de conseguir el mismo objetivo de forma artificial.

La solución obvia es construir una planta cuyas semillas sean estériles. Hay, sin embargo, un pequeño problema técnico. En el caso de cultivos híbridos, fertilizas la variedad A con la variedad B, produces muchas semillas híbridas y las vendes. Producir una semilla transgénica es un proceso más difícil y elaborado, que tiene mucho de ensayo y error en el camino de obtener un solo éxito. Si con todo lo que acabas es con una semilla que produce una planta cuyas semillas sean ellas mismas estériles, vas a pasarlo mal pagando el laboratorio.

La solución es construir genéticamente una semilla que produzca una planta cuyas semillas sean fértiles, pero que puedan modificarse, mediante la aplicación de la química adecuada, para producir una planta cuyas semillas sean estériles. Cultivas las suficientes

generaciones de la planta para producir la cantidad de semillas que quieras. Entonces tratas esa semilla y la vendes. Los agricultores la cultivan, obtienen su cultivo, pero no pueden volver a plantar, porque las semillas de las plantas cultivadas a partir de la semilla tratada son estériles. La compañía de semillas no solo consigue retener el control de su propiedad intelectual, sino que también reduce el riesgo de producir accidentalmente supersemillas, ya que el polen que se desprende de la cosecha creada genéticamente se ha construido para producir semillas estériles.

Los opositores de la biotecnología agrícola, en un golpe propagandístico brillante, llamaron a la invención patentada el «gen exterminador». Argumentaron que evitar que los agricultores volvieran a plantar de su propia semilla los convertiría en siervos bajo las compañías de semillas. Nunca se dejó completamente claro si pensaban que todos los agricultores que cultivaban semillas híbridas ya eran siervos. Tampoco se explicó cómo dar a los agricultores la opción de sembrar cultivos transgénicos y comprar semillas cada año o sembrar cultivos convencionales y plantar sus propias semillas les dejaba en peor situación que si solo hubieran tenido la última alternativa.

Críticos más responsables señalaron posibles efectos secundarios. Piensa, por ejemplo, en un campo de algodón ordinario plantado junto a uno de algodón genéticamente modificado. Parte del algodón ordinario se contamina por el algodón modificado, produciendo semillas estériles. El agricultor intenta volver a plantar a partir de su algodón ordinario, como tiene todo el derecho a hacer, y obtiene un rendimiento decepcionantemente bajo.

Por el momento, parece que los opositores han ganado. Sea por malos argumentos, buenos argumentos o propaganda astuta (¿quién, después de todo, quiere defender a un gen exterminador?), parece que han persuadido a las compañías de semillas de que abandonen esta solución en particular para proteger la propiedad intelectual. ¿Seguirá abandonada? Tendremos que esperar a ver qué pasa.

SATÁN ALADO

Hemos invertido algo de tiempo tratando de las malas consecuencias no intencionadas de la ingeniería genética. También hay intencionadas: guerra biológica que usa enfermedades a medida o, más modestamente, malas hierbas a medida. Aquí merece la pena de nuevo dar un paso atrás para pensar en las implicaciones de la biología evolutiva. Es un error considerar las enfermedades mortales como enemigos que están ahí fuera para destruirnos. Una bacteria de una plaga no solo no tiene nada contra ti, tiene los mejores deseos para contigo, o los tendría si fuera capaz de desear. Es un parásito, eres un huésped, y cuanto más vivas, mejor para él.

Las enfermedades letales son parásitos mal diseñados. Por eso una enfermedad que es realmente mortal es típicamente nueva, o una nueva mutación, una vieja enfermedad que infecta a una población que todavía no ha desarrollado resistencia, o una enfermedad que acaba de saltar de una especie a otra y todavía no se ha adaptado al cambio. Con el tiempo, la evolución funciona no solo para hacernos menos vulnerable a una enfermedad letal, sino para hacer la enfermedad menos letal para nosotros.[109]

Por desgracia, la creación de enfermedades letales ya no se limita a la naturaleza. Hace varios años, un grupo de científicos anunció[110] que habían conseguido recrear el polio. De cero. Las tecnologías relevantes están mejorando rápidamente, junto con la mejora general de la biotecnología. Podría no pasar mucho tiempo antes de que alguien que quiera comenzar una nueva plaga de viruela o apuntar a enemigos con ántrax necesitará solo unas herramientas apropiadas para la biosíntesis y una descripción completa del organismo.

Cuando un villano de James Bond tiene la intención de crear una enfermedad que matará a cualquiera salvo a sí mismo y su harén, no está compitiendo con la naturaleza: la naturaleza, la evolución darwiniana, no está tratando decrear enfermedades mortales. Eso hace más probable que triunfe, más probable que haya formas de hacer más mortales las enfermedades que las producidas por evolución natural. La

---

109 McNeill, 1978, y Oldstone, 1998.

110 http://www.newscientist.com/article.ns?id=dn2539.

cuestión entonces se convierte en si el progreso tecnológico que hace más sencillo diseñar enfermedades asesinas (en última instancia, quizás, en tu sótano) triunfa o no en la carrera con otras tecnologías que hacen más sencillo curar o prevenir dichas enfermedades. Es un caso especial de un asunto al que volveremos en el contexto de la nanotecnología, que ofrece proporcionar a los tipos malos potenciales un kit de herramientas aún más amplio para el asesinato masivo y podría o no proporcionarnos al resto de nosotros las herramientas necesarias para defendernos contra ellos.

Matar solo a la gente adecuada

La guerra biológica es un problema simple si eres un lunático que se dispone a acabar con el mundo, pero, puesto que los cambios tecnológicos que están haciendo más sencillo que se creen tecnologías también están haciendo más fácil que otra gente se proteja de ellos, es improbable que los lunáticos tengan suficiente competencia o recursos para hacer un buen trabajo. El peligro más serio viene de los proyectos de investigación, probablemente financiados por los Gobiernos, para producir enfermedades destinadas a matar solo a la gente «adecuada». Alcanzar ese objetivo plantea algunos problemas prácticos.

El caso sencillo es el que ya ha sucedido, varias veces. Si hay una enfermedad a la que tu población ya es resistente y la población meta no lo es, exponer a la población meta a esta enfermedad puede tener efectos drásticos. El ejemplo obvio es el efecto sobre la población del Nuevo Mundo de la exposición a las enfermedades del ViejoMundo; algunos historiadores estiman tasas de mortalidad de más del 90%.[111] En su mayoría, esta forma particular de guerra biológica fue un accidente, aunque parece haber al menos un caso histórico de expansión deliberada de viruela entre los indios canadienses de la que se informó en la correspondencia de los oficiales británicos.[112] William McNeill argumenta, en *Plagas y pueblos*, que las poblaciones civilizadas

---

[111] Los escritos sobre este asunto y otros relacionados se encuentran estudiados en Mann, 2005; hay una crítica en http://www.victorhanson.com/articles/thornton070206.html.

[112] Una discusión detallada del caso, incluyendo enlaces a imágenes de las cartas, se puede encontrar en http://www.nativeweb.org/pages/legal/amherst/lord jeff.html.

(definidas simplemente como las que tienen ciudades) tienen una ventaja en la bioguerra automática en su interacción con las no civilizadas, ya que las enfermedades letales requieren una población densa[113] para no extinguirse en el proceso de matar a sus huéspedes. Por tanto, las poblaciones densas serán las que lleven y sean resistentes a enfermedades nuevas y letales a poblaciones más dispersas.

En el mundo moderno, la movilidad humana es demasiado alta y las poblaciones densas demasiado comunes para que ese tipo particular de plaga selectiva sea una herramienta útil para los que se inclinen por el asesinato masivo. Sin embargo, hay dos variantes modernas que podrían funcionar mejor. La obvia es desarrollar una enfermedad, una vacuna, vacunar a tu propia población y luego soltar la enfermedad; un agresor prudente probablemente querría disfrazar el programa de vacunación como si estuviera diseñado contra algún peligro natural.

Otra alternativa, que requiere una tecnología más avanzada, sería diseñar una enfermedad específica para las víctimas con ciertas características particulares, unas que sean mucho más comunes en la población meta que en la tuya. Esto tiene la desventaja de que, dada la variabilidad genética humana, es probable que mate a muchos de tus propios ciudadanos. Pero uno puede imaginarse a un Gobierno dispuesto a aceptar ese coste o uno que no lo considerara un coste, según la teoría de que los ciudadanos demasiado relacionados con el enemigo genéticamente podrían no ser de fiar políticamente. Si parece implausible, piensa en el tratamiento de los japoneses-estadounidenses por parte de EE.UU. durante la Segunda Guerra Mundial.

Otra posibilidad sería apuntar a lugares más que a gente. Ello significaría diseñar una enfermedad que se extendiera fácilmente en el ambiente físico de la nación enemiga, pero no en tu ambiente más frío o cálido, más húmedo o seco. Podría significar una enfermedad diseñada para extenderse tras un cierto número de generaciones, usando una versión más sofisticada de la solución del gen exterminador. Haz que arranque en medio del país enemigo, cierra tus aeropuertos y puertos durante una semana para mantener fuera a los viajeros que puedan ser portadores, y con suerte mata a una gran

---

[113] Si no, una enfermedad letal puede existir en un ambiente lo bastante cálido y húmedo para permitir la supervivencia durante un tiempo considerable fuera del húesped.

fracción de la población enemiga mientras que dejas su tierra y fábricas sin tocar para tu uso y tu propia población sin daños.

Siempre que la enfermedad no consiga, durante sus generaciones asignadas, evolucionar hasta quedar libre del gen exterminador.

DIECISÉIS

DROGAS MENTALES

MEJOR VIVIR A TRAVÉS DE LA QUÍMICA

Al menos desde el descubrimiento del alcohol, los humanos han usado drogas para afectar a la mente. A medida que aprendemos más sobre cómo funciona esta y nos volvemos más hábiles en la síntesis química, podemos esperar mejorar en ella. Será algo positivo de muchas maneras: las drogas ya proporcionan beneficios sustanciales a algunos que sufren de desórdenes mentales. Pero, como la mayoría de las tecnologías nuevas, es probable que las drogas mentales mejoradas también planteen nuevos problemas legales, sociales y personales.

Para los propósitos de este capítulo, será útil pensar en cuatro clases distintas de drogas mentales: placer, actuación, personalidad, control. Algunas drogas encajarán en más de una categoría, con lo que reflejarán múltiples razones de por qué se usan.

Piensa en el familiar caso del alcohol. Alguna gente lo bebe porque les gusta cómo les hace sentir: placer. Algunos lo beben porque creen que mejora su actuación: un conocido, cuando era estudiante universitario, tomaba por rutina media lata de cerveza antes de un examen. Algunos piensan que proporciona un cambio temporal en su personalidad que a veces desean. Y alguna gente suministra alcohol a otra, a veces sin su conocimiento, como una forma rudimentaria de controlarla.

Placer y felicidad

¿Cómo podría encontrarse descrita en la literatura una droga de felicidad eterna, una droga que (¡de forma implausible!) dejó a alguien que la probó una vez viviendo feliz por siempre jamás? La sustancia x induce dañoestructural severo e irreversible al subsistema neurotransmisor y. Sus secuelas incluyen alucinaciones cognitivas

congruentes con el estado de ánimo, euforia resistente al tratamiento y psicosis afectiva tóxica.

www.biopsychiatry.com/

En la mayoría de los contextos consideramos buenos la felicidad y el placer. Jeremy Bentham, uno de los filósofos más influyentes del siglo XIX, ofreció un estándar simple para juzgar todo: su efecto sobre la utilidad, felicidad, el exceso de placer sobre el dolor en la vida humana. Cualquier cosa que incrementara la utilidad era buena; cualquiera que la disminuyera, mala.

Muchos de los productos químicos consumidos para incrementar su utilidad son ilegales. Los que apoyan las leyes contra las drogas recreativas basan su apoyo en una variedad de afirmaciones basadas en hechos, algunas ciertas, algunas falsas. No es cierto que fumar marihuana enloquezca a la gente y cometan crímenes violentos, como se afirmaba en *Reefer Madness*, una película que representó un importante papel al inspirar la legislación antimarihuana original. Es cierto que la gente bajo los efectos del LSD frecuentemente no es capaz de realizar tareas ordinarias como conducir un coche de forma segura o mantener una conversación coherente, y es cierto que algunas drogas tienen efectos desfavorables a largo plazo en algunos consumidores.[114]

Si las afirmaciones negativas de algunas o todas las drogas recreativas actuales son o no ciertas, es improbable que sean ciertas para todas las drogas recreativas futuras. Cuanto más sabemos sobre cómo funciona la mente humana, mejores nos volveremos creando drogas que proporcionen placer sin efectos negativos serios. A menos, por ejemplo, que el placer mismo sea el problema. Posiblemente podría serlo. La evolución es un bioquímico extraordinario, mucho mejor que nosotros produciendo compuestos que afecten a las criaturas vivas de formas útiles. Si podemos crear un producto químico que nos produzca placer, y el placer es bueno, ¿por qué no venimos ya equipados para obtener el placer que pidamos?

La respuesta obvia es que estamos diseñados por la evolución no para la felicidad, sino para el éxito reproductivo. El placer y el dolor

[114] Para información razonablemente objetiva sobre las drogas, véase Rosen y Weil, 2004, y la página web de Erowid, http://www.erowid.org/.

proporcionan incentivos para actuar de formas que cumplan ese objetivo: que nos pongamos a tener relaciones sexuales, que quitemos las manos de los hornos calientes. Presumiblemente hay algún equilibrio óptimo, algún nivel normal que permita la suficiente desviación en una dirección para proporcionar un incentivo adecuado para hacer cosas que vayan en la dirección de los intereses de los genes y lo suficiente en la otra para que hagan que evitemos cosas contrarias a esos intereses.

Si las drogas del placer son demasiado buenas, podrían interferir no solamente en el éxito reproductivo, sino con la supervivencia física. Larry Niven proporciona un ejemplo ficticio[115] en forma no de una droga, sino de estimulación eléctrica directa del centro de placer del cerebro. Sus «yonquis» son capaces de conectarse y morir de hambre, porque un minuto más de placer intenso vale más para ellos que la comida o bebida. Si aceptamos ese argumento, la implicación no es que las drogas que proporcionan placer son malas, sino solo que deberían usarse con moderación. No se sigue que siempre vayan a serlo.

Para un ejemplo menos exótico, piensa en una droga placentera incluso más respetable que el alcohol: la humilde tableta de chocolate. Si tienes gustos más elevados, conviértela en una cena en un restaurante de cuatro estrellas en París. La comida, después de todo, se consume en gran parte para darnos placer sensual. Una dieta de coste mínimo completamente nutritiva, basada en harina, mantequilla de cacahuete, repollo y otros ingredientes altamente nutritivos, vale menos de dos dólares al día.[116] El resto de lo que gastamos es por placer.

El problema del mundo real de hoy de cambiar al placer a corto plazo en lugar de metas más importantes a largo plazo es, seguramente, no la inanición del yonqui de Niven, sino su contrario: la obesidad. La gente

---

[115] Los yonquis aparecen en una serie de historias de Nivel, incluyendo "Muerte por Éxtasis", en Niven, 1969.

[116] Los cálculos originales, pasados de moda hace mucho, estaban en Stigler, 1945. Una versión actual, para los precios de 1998 y RDA, está descrita en Gass yGarille, 2001, en http://solstice.uwaterloo.ca/~phcalama/Courses/SD311/Project/Group18/Group18paper.pdf, un fragmento de la cual traducimos aquí: «El problema actualizado muestra que la dieta óptima para un hombre entre 25 y 50 años consiste diariamente en unos 0,33 litros de harina de trigo, 0,332 de copos de avena, 473 ml de leche, 57,9 g de mantequilla de cacahuete, 109,2 g de manteca de cerdo, 0,028 g de hígado de ternera, 50 g de plátanos, 2,2 de naranja, 0,16 l de repollo, 0,07 de zanahoria, 0,072 de patata y 0,02 de cerdo y judías. El coste diario de esta dieta es de 1,78 dólares.»

disfruta comiendo. Las sociedades modernas son lo bastante ricas para que casi todos puedan permitirse consumir tantas calorías como quieran, una observación confirmada por media hora invertida en observar a gente de un vecindario de renta baja.[117] Un resultado es que un número creciente de gente, en EE.UU. y otras partes, tiene kilos de más, pesan lo bastante para, según pruebas actuales, que llegaran a vivir más si comieran menos.

Un argumento más general contra las drogas placenteras es que el simple placer no es todo lo que importa, como sugieren no solo los filósofos, sino el comportamiento observado. Pocas parejas practican el sexo tan frecuentemente como sería físicamente posible; pocos individuos solteros se masturban tan frecuentemente como sería físicamente posible. Si imaginamos a alguien que pasa la mayoría de su vida en un aturdimiento inducido por las drogas, podríamos sospechar que, por muy intenso que sea el placer, no es realmente feliz.

Esto sugiere la respuesta menos interesante a la posibilidad de las drogas placenteras: que no funcionan, que sean cuales sean sus beneficios a corto plazo, a la larga son una trampa y una ilusión. Que yo sepa, esto podría ser cierto para las drogas recreativas que se encuentran ahora en el mercado, aunque deduzco que muchos consumidores discrepan. Pero es muy irrelevante si pensamos en el futuro.

Felicidad

Troy Dayton se toma una pequeña pastilla blanca cada mañana. Es uno de los diez millones de estadounidenses que se toman un antidepresivo diario. Pero en su caso, dice que nunca estuvo deprimido.

Este miembro de un grupo de presión política, de veintinueve años, es una de las personas más felices que jamás vas a conocer.[118]

---

[117] El equivalente estadístico más riguroso encuentra la obesidad más común en los estadounidenses de menor renta, pero no por mucho; http://paa2006.princeton.edu/download.aspx?submissionId=60728.

[118] http://www.cnn.com/2006/HEALTH/conditions/11/13/unnatural.highs/index.html, CNN, November 17, 2006.

Quizás el placer, en el sentido de la heroína y tabletas de chocolates, es una meta demasiado estrecha. Puesto que no estamos limitados a la tecnología actual, reemplaza el placer por la felicidad, el estado mental en el que consideramos el placer como una inversión. Piensa, no en el yonqui de Niven, sino en la persona más feliz que conozcas.

Mi candidato es una compañera profesora de derecho que posee lo que me gusta describir como una personalidad que brilla en la oscuridad. Años después de que la conociera, me di cuenta de una vieja fotografía en un estuche de la facultad de derecho que mostraba a un profesor destacado recibiendo un premio de los estudiantes. La figura central de la foto, la cara que sobresalía del resto, no era el que recibía el premio, sino la estudiante que lo daba. Era una cara conocida.

Es posible, por supuesto, que la felicidad de esa gente refleje el hecho de que tienen mucho por lo que estar felices: una esposa cariñosa, hijos, un trabajo satisfactorio, ninguna de las cuales es una cosa que pueda proporcionar una droga. Pero no parece ser todo. Los estudios de felicidad muestran que la gente feliz sigue feliz incluso cuando cambian las circunstancias, al menos una vez han tenido tiempo para ajustarse a los cambios. Se me recordó ese resultado no hace mucho, en una conmemoración para un amigo que había muerto hacía un poco menos de un año. Su viuda estaba allí. Había sido un matrimonio feliz y largo. Pero nadie que no conociera los hechos, observándola, se habría dado cuenta de que había perdido recientemente al hombre que amaba. También ella, creo, es una persona naturalmente feliz.

Así que piensa, no en una droga para el placer, sino para la felicidad, una diseñada para modificar la química de tu cerebro de forma que seas más como mi amiga que brilla en la oscuridad. Si pudieras, ¿lo harías? ¿Deberías? La respuesta posible es que una felicidad así es antinatural. De nuevo el argumento es que hemos sido diseñados por la evolución, y la evolución es mucho mejor en neuroquímica que nosotros. Si la química cerebral que nos hace felices fuera buena, todos la tendríamos ya. El argumento ya ofrecido para el placer puede reutilizarse para la felicidad. También puede verse como un premio programado en nosotros para el comportamiento que aprueban nuestros genes. Seguramente es difícil que nuestros genes sobornen con felicidad a

gente que ya es feliz. Mientras que la evolución podría ser muy buena en bioquímica, sus objetivos no son los mismos que los nuestros. Desde el punto de vista de la evolución, simplemente somos maquinaria con la que los genes hacen otros genes. El objetivo del diseño es el éxito reproductivo, la capacidad para incrementar la frecuencia de nuestros genes en generaciones futuras.

Ese podría no ser el objetivo de mi diseño para mí; si lo fuera, tendría más de tres hijos. No parece ser tampoco el objetivo de mucha otra gente; si lo fuera, los hombres pagarían cantidades sustanciales para que se les permitiera donar en bancos de esperma y las mujeres que vendan sus óvulos lo harían a un precio negativo más que positivo. Después de todo, que otro conciba y críe a nuestros hijos es una forma extraordinariamente barata de extender los genes.

No solo la evolución tiene el objetivo erróneo: sus diseños también están pasados de moda. Los humanos tienen generaciones largas y, por tanto, evolucionan lentamente. Las pruebas que tenemos sugieren que estamos adaptados no a las circunstancias actuales, sino a las sociedades de cazadores-recolectores en que nuestra especie pasó la mayor parte de nuestra existencia. Incluso si una personalidad demasiado feliz es normalmente un estorbo en la sociedad cazadora-recolectora, y muy rara, podría no serlo en una sociedad moderna. La gente feliz que conozco parece apañárselas muy bien por sí mismos.

Una segunda objeción, más interesante, es que el utilitarismo es malo, que la felicidad no es todo lo que importa. Para hacer más plausible esa objeción, piensa en dos vidas alternativas que podría vivir. Una es la vida que he vivido. Ha sido, en conjunto, feliz. También ha producido una serie de cosas que valoro: un matrimonio feliz, tres hijos y media docena de libros, de todos los cuales estoy orgulloso, una variedad de ideas en varios campos relacionados y muchas otras cosas que soy demasiado modesto (o vago) para mencionar.

La otra es la vida que podría haber vivido si tuviera drogas adecuadas, suficientes para hacerme en cada momento de esa vida al menos tan feliz como en la vida que tuve. Es cierto que en esa vida no habría tenido los placeres de hijos, niños y otros logros. Pero se me habría compensado por esa falta mediante un incremento artificial en la química cerebral que conecta la causa del logro con el efecto de la

felicidad. ¿Qué vida merece más la pena vivir? Esa es una pregunta a la que volveremos en un capítulo posterior, en el contexto de la realidad virtual, otro atajo posible hacia la felicidad.

Si bien es una pregunta interesante, podría no tener mucha relevancia con respecto al efecto de las drogas de la felicidad (entendidas como las opuestas al placer). Juzgando al menos por observación desinteresada, los procesos que producen el equivalente natural de las drogas de la felicidad no evitan que los que se beneficien de ellas vivan vidas activas y productivas.

La historia de la CNN del uso de Troy Dayton de Wellbutrin como droga de la felicidad contenía una variedad de advertencias extremas:

Los psiquiatras dicen a la CNN que el uso que Dayton realizaba del Wellbutrin como parte de su estilo de vida es potencialmente peligroso, aunque se sabe poco de sus efectos a largo plazo. «Esas medicinas no son inocuas», opina el Dr. Peter Kramer, autor de *Escuchando al Prozac*. Kramer afirmó que algunos médicos piensan que si sigues usando antidepresivos el suficiente tiempo, acabarás dependiendo de ellos. Otros médicos creen que podría desencadenar enfermedades maniaco-depresivas en gente propensa, contó dicho doctor.

La historia no ofrece ninguna prueba real de daño. La droga funciona incrementando el nivel de serotonina, una sustancia neuroquímica asociada con sentirse bien: «Químicamente, hay poca diferencia entre sentirse bien por medicación y sentirse bien de forma natural».

Actuación

Preferiría que mi hijo tomara esteroides anabolizantes y hormonas de crecimiento antes que jugara al rugby. La hormona de crecimiento es más segura. Al menos no conozco ningún caso de cuadriplejia causado por una hormona del crecimiento.

Julian Savulescu, profesor de ética práctica en Oxford[119]

---

[119] Citado en http://www.trebach.com/drugwar/ChemicallyEnhanced.html; Savulescu, Foddy, and Clayton se encuentra en http://bjsm.bmj.com/cgi/content/extract/38/6/666.

Las drogas de actuación que actualmente son un problema público tienen que ver con el cuerpo, pero plantean muchos de los mismos temas que las drogas para mejorar la actividad mental. Todo el mundo parece estar de acuerdo en que es malo que los atletas usen esteroides, pero no está completamente claro el porqué. Después de todo, los atletas han estado usando dieta y ejercicio para mejorar su actuación durante miles de años, así como una variedad de drogas más viejas. ¿Por qué de repente se vuelve pecaminoso el proceso cuando se cambian a los esteroides?

Una respuesta es que, ya que el uso de esteroides está prohibido actualmente, los que usan esteroides están obteniendo una ventaja injusta. Pero eso no explica por qué están prohibidos actualmente cuando no lo están otras formas de conseguir ventaja. Una segunda respuesta es que tenemos miedo de que los jóvenes atletas, con una preocupación inadecuada por su propio futuro, se hagan daño de verdad en el proceso de intentar ganar. Pero mientras que tomar esteroides podría reducir la esperanza de vida (las pruebas parecen ser mucho más débiles de lo que sugieren las discusiones populares[120]), también lo hace conducir un coche en una pista a algo más de trescientos kilómetros por hora, algo que se le permite hacer a los jóvenes pilotos de carreras. ¿Por qué nuestro paternalismo es tan selectivo?[121]

La respuesta más interesante, al menos para un economista, es que nuestra oposición surge de la naturaleza especial del producto que fabrican las competiciones deportivas. Posiblemente, de lo que nos preocupamos sobre todo es de la capacidad relativa, no absoluta, de los atletas. Una carrera en la que un competidor alcanza algo más de un kilómetro y medio en cuatro minutos y el otro en tres minutos cincuenta y nueve segundos es tan emocionante como uno en el que los

---

[120] Para una discusión mucho más detallada, véase Mehlman, Benger y Wright, 2005.

[121] Otra respuesta que se ha ofrecido es que los atletas del presente están compitiendo contra los del pasado, intentando superar sus marcas. Los atletas del pasado no tenían acceso a esteroides, así que el uso de ellos que hacen los atletas de ahora es competición injusta. Los atletas pasados tampoco tenían equipo deportivo reforzado por fibras de carbono, entrenamiento moderno y regímenes de dieta, y una variedad de cosas que los atletas de ahora sí tienen, pero quizás esa es la única ventaja que esperamos ser capaces de controlar.

tiempos son 3:59 y 3:58. Queremos que nuestro equipo de béisbol favorito juegue un poco mejor que sus oponentes, pero nos importa poco el nivel absoluto en el que juegan. En tanto que esta afirmación sea cierta (algunos aficionados al deporte lo discutirían), la competición con uso de esteroides es un error. Ambos equipos, boxeadores o corredores se vuelven un poco mejores, su capacidad relativa no se ve afectada, los aficionados no están más contentos y los atletas mueren un poco más jóvenes.

Piensa ahora en el equivalente mental de los esteroides. El Ritalin, por ejemplo, se considera por lo general como medicación para el Trastorno por Déficit de Atención (TDA). Sin embargo, resulta que uno no puede decir si alguien tiene TDA dándole Ritalin y viendo si mejora su concentración, porque el Ritalin mejora la concentración de todo el mundo. Se sigue que a alguien que quiere hacerlo bien, digamos, en un examen, se le podría avisar y que obtuviera de alguna forma algo de Ritalin para tomárselo antes de entrar en el examen, y deduzco que algunos lo hacen. Hay información de que otras drogas obtenidas ilegalmente, como las anfetaminas, son de uso común para propósitos similares. Quizás cuando se aproxima la fecha de entrega de un trabajo, un estudiante dado al retraso podría querer obtener algún modafinilo,[122] una droga que parece eliminar la necesidad de dormir durante periodos sustanciales de tiempo y que, si se pueden creer las noticias, actualmente se usa en el ejército estadounidense para ese fin.

Un argumento para prohibir el uso de esas drogas por parte de los que se presentan al examen del colegio de abogados, o a Selectividad, o a un examen de fin de carrera, es que distorsionen la información que produce el examen. Una empresa de derecho que está decidiendo si contratarte no quiere saber lo buen abogado que eres cuando estás bajo la influencia del Ritalin, a menos que esperen que sigas consumiéndolo regularmente durante el resto de tu vida como trabajador. Quieren

[122] Los estudios de los militares estadounidenses descubrieron que los soldados pueden permanecer despiertos y estar en alerta durante cuarenta horas, dormir ocho horas y luego permanecer despiertos cuarenta horas más, todo sin el juicio debilitado de los estimulantes anticuados. http://www.modafinil.com/article/soldiers.html. También hay pruebas de que la droga aumenta las capacidades mentales de otras maneras: http://www.futurepundit.com/archives/000534.html.

saber lo buen abogado que eres bajo las condiciones en que estarás trabajando.

Esto tiene sentido siempre que solo estemos hablando de efectos temporales. La cuestión se vuelve más interesante si pensamos en una droga que se puede administrar de forma regular, como la gente a la que se le ha diagnosticado TDA que use Ritalin, o una que produzca efectos a largo plazo en vez de a corto. Entonces tenemos el equivalente mental de un esteroide.

Parte de la hostilidad contra el uso regular de esas drogas, como con los esteroides, se basa en la idea de que lo que están haciendo es ayudar a que el usuario gane una competición, no en el campo de juego sino en el mercado de trabajo. Si ambos competidores usan la droga, nadie gana ninguna ventaja relativa y ambos están peor por los costes que tenga la droga, sea en dinero o salud.

Ese argumento refleja un malentendido fundamental de la competición económica. Si tú y yo somos corredores y ambos usamos esteroides, los dos corremos un poco más rápido y aun así tú ganas la carrera. No se ha ganado nada, y, si los esteroides tienen efectos secundarios indeseables, se pierde algo. Pero si tú y yo somos carpinteros de viviendas que usamos una versión mejorada de modafinilo para aumentar el trabajo y el ocio, trabajando diez horas de cada veintidós en vez de ocho de cada dieciséis, el resultado es que se construyen más casas. El beneficio último podría ir a nosotros en forma de más ingresos de nuestra mayor productividad y más ocio para disfrutarlos. Podría ir a las gentes que compran casas, si nuestros resultados mejorados bajan el precio de nuestros servicios. Podría dividirse entre nosotros y nuestros clientes. Los detalles de lo que sucede dependen de los detalles del mercado de nuestros servicios. Pero en todos los resultados, el tiempo extra que hemos obtenido reduciendo drásticamente nuestro tiempo de sueño, o la calidad superior de mejorar nuestra capacidad de prestar atención, está produciendo un beneficio real a alguien, no solamente una ventaja competitiva.

El argumento se aplica donde quiera que importen los resultados absolutos y no simplemente relativos, lo que significa casi en cualquier parte. «Competición» es un término engañoso porque sugiere que,

como en los deportes, todo cuanto importa es quien gane. Las granjas no existen para ganar una competición, sino para producir comida. Los carpinteros no existen para ganar una competición, sino para construir casas y sillas y meses. Las drogas que nos hacen estar más alerta, o ser más astutos, o proporcionarnos mejores recuerdos, o reducir la necesidad de dormir, nos dejan hacer mejor lo que sea que estemos haciendo. Eso es un beneficio neto que se debe sopesar con los costes asociados con el uso de la droga.

¿Nos dan las drogas mejores recuerdos? Todavía es una pregunta abierta, una íntimamente asociada con el intento de reducir la pérdida de memoria por párquinson. Pero hay una buena razón para creer que esas drogas existirán, y al menos alguna razón para creer que ya sabemos de drogas que mejoren la memoria hasta cierto punto. La misma afirmación se realiza a veces respecto a la inteligencia: que ahora existen «drogas para la astucia». Existan o no, parece probable que lo harán.

Podría ocurrírseles a algunos lectores que el argumento que me he ofrecido a explicar concierte a drogas de mejora, por muy entretenido que sea para un economista, se pasa de listo, ya que la mayoría de la gente ordinaria no distingue entre actividades puramente competitivas y actividades productivas. Una explicación posible y que proporciona al menos una explicación parcial de la hostilidad hacia muchas tecnologías diferentes, es que la gente es simplemente conservadora, escéptica hacia lo nuevo, «antinatural», a pesar de la naturaleza antinatural de casi todo lo que comemos, bebemos o vestimos actualmente.

Como prueba, ofrezco el siguiente comentario sobre el modafinilo de un médico que trata desórdenes de sueño: «Creo que el sueño es bueno. Lo saludable es dormir más si estás cansado, ¿no?»[123]

Una conjetura convertida en hecho frente a tus mismos ojos.

[123] http://www.modafinil.com/article/soldiers.html de *The Ottawa Citizen*,11 de octubre, 2003.

Personalidad

Anteriormente en este capítulo planteé la cuestión de si la oportunidad de experimentar placer podría hacernos estar peor en vez de mejor. Un ejemplo es la obesidad. Peso más de lo que creo que debería, aun así lo paso mal perdiendo kilos. Como mucha otra gente, puedo resistirme a cualquier cosa salvo a la tentación. A medida que desarrollemos formas de obtener fácilmente placeres mucho más intensos, hay algo de riesgo de que podamos sentirnos tentados a abandonar los beneficios a largo plazo a cambio de los de a corto, incluso cuando no deberíamos. Esto plantea una pregunta obvia: ¿qué significa «no deberíamos»? ¿Cómo, más allá de observar las decisiones que toma la gente, podemos juzgar sus valores? ¿Qué quiero decir si afirmo que hice una cosa pero debería haber (en cierto modo, realmente quería) hacer otra?

Una respuesta a esa pregunta que encuentro intuitivamente atractiva es pensar en mí como dos personas en una, un planificador a largo plazo y un maximizador de la utilidad actual a corto plazo. El planificador utiliza dispositivos como la culpabilidad y los compromisos para intentar manipular al maximizador a corto plazo, el yo que tiene control real de mi cuerpo. Podría decidir (haber decidido de vez en cuando) que no me permitiré tomar helado como postre hasta que haya conseguido que mi peso baje de un cierto nivel arbitrario. Podría decidir (de hecho lo decidí, no mucho antes de escribir estas palabras) fijar un límite de resultados más bajo para lo que escribo al día, un número de palabras que debo producir antes de permitirme ir a la cama o consentirme jugar al *World of Warcraft*. A veces los dispositivos confían en ayuda externa, como cuando un empleado hace arreglos para que se transfiera automáticamente cada mes una cierta cantidad de sus ingresos en una cuenta de ahorro.

Esta forma de mirarlo sugiere una posibilidad intrigante. Quizás el problema de las drogas del placer podría tratarse con las drogas de la personalidad. Alguna gente parece tener un horizonte temporal más largo que el de los otros, ser más capaz de controlar su deseo de placer inmediato para lograr mejor sus metas a largo plazo. Quizás, a medida que aprendamos más sobre cómo funciona el cerebro, descubriremos

que la diferencia refleja alguna diferencia en la química cerebral. Quizás las drogas para la personalidad acabarán situando al planificador a largo plazo en un segundo plano.

Piensa, por ejemplo, en lo que sabemos ya de los efectos de la dopamina, un neurotransmisor que representa un papel importante en la química cerebral. Una carencia de dopamina en el cerebro tiene como resultado una personalidad indecisa; el párquinson es una versión extrema. Los ratones con un exceso de dopamina cerebral, por el contrario, son muy exploradores y arriesgados. Todavía no sabemos con detalles los mecanismos que producen esos resultados, pero al menos demuestran que esa personalidad depende en parte de la química cerebral.

Para un resultado más impactante debido a una alteración más drástica del cerebro, piensa en la anécdota más famosa de este campo: la triste historia de Phineas P. Gage. Como resultado de un descuido momentáneo con los explosivos en 1848, una varilla de metal de más de un metro le atravesó la cabeza y le dejó un agujero en su cubierta ósea por el que el médico que le atendía podía meter todo su dedo índice. Sorprendentemente, se recuperó de la herida en unas pocas semanas y volvió a su trabajo como capataz de un grupo de voladura para construir ferrocarriles. «No tenía ningún déficit intelectual aparente o pérdidas de memoria. Aun así, su vuelta al trabajo mostró rápidamente la naturaleza del déficit que sigue a un gran daño del lóbulo frontal. El capataz, anteriormente de modales suaves, reflexivo y dispuesto a cooperar, se había transformado en un tirano de malas palabras y beligerante. Perdió su trabajo, se unió a un espectáculo itinerante durante unos pocos años para capitalizar (con pequeñas sumas) su desgracia, y murió de un ataque epilépticos unos trece años más tarde»[124]

Si se pueden usar drogas para la personalidad con el fin de proporcionarnos personalidades mejores que la media o no, actualmente se están usando para tratar con personalidades percibidas, por los que las poseen u otros, como peores de la media. El trastorno

---

[124] De C. Robin Timmons y Leonard W. Hamilton, *Drogas, el cerebro y el comportamiento,* en: http://www.rci.rutgers.edu/~lwh/drugs/chap02.htm, basado en gran parte en Timmons y Hamilton, 1990.

bipolar es un ejemplo, la depresión es otro. Ambas pueden verse como trastornos de personalidad. Ambas se tratan con drogas, al menos en algunos casos con éxito aparente.

Control

Las golosinas son estupendas, pero el alcohol es más rápido.

Hasta ahora hemos estado considerando cosas que podríamos ser capaces de hacernos a nosotros mismos mediante el uso de drogas. Sigue quedando el asunto de las cosas que otra gente podría hacernos. Dos ejemplos obvios son las drogas que dejan inconsciente a la víctima: el hidrato de cloral, el «Mickey Finn» de las viejas historias de detectives, y sus equivalentes más modernos (y el uso de alcohol como ayuda a la seducción). Drogas más nuevas podrían servir para el mismo propósito. Un efecto del éxtasis (MDMA) es hacer al usuario más cálido, más empático. En la mayoría de las circunstancias, es un efecto deseado, un ejemplo del uso de una droga para cambiar la personalidad de uno. Pero también es una razón por la que un hombre podría darle la droga a una mujer a la que está intentando seducir.

Como sugiere este ejemplo, la diferencia entre las drogas para la personalidad y las de control no depende tanto de la naturaleza de la droga como de cómo se usen. Una mujer que se emborracha para dejarse seducir está usando el alcohol para alterar temporalmente su personalidad. Un hombre que emborracha a una mujer para el mismo fin está usándolo para controlarla.

La gama de drogas de control actualmente está muy limitada. Hay drogas para dejar sin conocimiento. Hay drogas que inducen amnesia temporal, como el Rohypnol, a veces llamado la droga de la violación en las citas. Hay drogas como el alcohol y la marihuana que relajan a la gente y hacen más difícil que piensen claramente. Eso es todo.

Sin embargo, hay pruebas en el horizonte de que habrá más. Una serie de experimentos extraños acerca de la reacción de alguna gente a oler la transpiración de otra gente sugiere que podría haber feromonas humanas, componentes que hagan que alguien huela de forma atractiva

para otra persona; quizás algún perfume funciona de verdad.[125] Si podemos aislar esos componentes y dar con cómo funcionan, podríamos ser capaces de producir los mismos efectos de forma mucho más poderosa. Los afrodisiacos de hoy podrían ser sobre todo un mito, pero siempre hay un mañana.

Aún más inquietante es la posibilidad de drogas que hagan crédulo al consumidor, dispuesto a creer lo que se le diga, o que le hagan obediente, o leal. Hay cierta evidencia de que la oxitocina tiene ese efecto.

Para experimentar cómo podría funcionar una droga para la lealtad, piensa en el Mulo, un personaje en la trilogía *Fundación*, de Isaac Asimov, una vieja y famosa obra de ciencia ficción. El Mulo tiene un simple talento: la habilidad para hacer que la gente quiera servirle. Lo usó para construir un imperio interestelar. Sus sirvientes sabían perfectamente que eran leales porque había usado su habilidad especial para que lo fueran, pero no les molestaba. Servir al Mulo era lo mejor que podían hacer, así que ¿por qué molestarse por el hecho de que les hubiera hecho querer hacerlo?

Esto es solo ciencia ficción, pero hay un equivalente en el mundo real que todos nosotros hemos observado y muchos hemos experimentado: el sentimiento de los padres hacia sus hijos. Los padres aman a sus hijos y desean servirlos y protegerlos, no porque el padre haya hecho un juicio objetivo sobre lo que merecen sus hijos, sino porque los padres han sido programados por sus genes para sentirse así, mediante mecanismos, algunos de los cuales bien podrían ser químicos. Los padres que resultan ser biólogos evolutivos saben que sus hijos los tienen cogidos por los genes y por qué; aun así, se sienten igual.

Descendemos de gente que no solo produjo hijos, sino que cuidó lo suficientemente bien de ellos para que llegaran a la madurez y se reprodujeran; hemos sido seleccionados, durante un periodo mayor de lo que ha existido nuestra especie, para la característica de altruismo hacia nuestros hijos. Pero esa explicación evolutiva no nos dice nada del mecanismo subyacente, como la observación de que ser capaces de ver

---

[125] Spencer, McClintock, Sellergren, Bullivant, Jacob, y Mennella, JA, 2004. Véase también http://pheromones.com/professional.html.

hace mucho más fácil la supervivencia no nos dice nada sobre cómo funciona el ojo. Si pudiéramos aprender a entender el mecanismo, la naturaleza de los cambios internos que sustentan el mecanismo, la naturaleza de los cambios internos que apoyan el amor parental, podríamos ser capaces de usar ese conocimiento para hacer que los otros nos amen como si fuéramos sus hijos. Lo mismo para el amor romántico, que produce efectos similares de algunas maneras.

Acabamos de aproximarnos a la capacidad para hacer este tipo de cosa, pero hemos estado pensándola mucho tiempo. Piensa en el *Orlando Furioso* de Ariosto, una obra del siglo XVI de fantasía cuyos personajes pasan el tiempo caminando por un vasto bosque que parece extenderse desde Inglaterra hasta China: la geografía no era una de las preocupaciones de Ariosto.

El bosque está bien abastecido de estanques y manantiales para el uso de aventureros sedientos. Que yo recuerde (leí el libro hace mucho), hay tres tipos distintos. Beber del primero elimina la memoria. Beber del segundo provoca odio hacia el ser que más se ame. Beber del tercero provoca enamoramiento hacia la próxima cosa viviente que se vea. Para Ariosto solo eran un mecanismo útil para la trama, una forma de meter a sus personajes en situaciones entretenidas y divertidas. Ya tenemos versiones del primer manantial: el Rohypnol, por ejemplo, aunque su efecto es más breve. El resto podría estar llegando.

Supón que desarrollamos drogas de control mucho mejores; ¿cómo podrían ajustarse nuestras leyes e instituciones? Una posibilidad es un régimen legal bajo el cual un contrato sea vinculante solo si ambas partes se han sometido a una prueba justo antes de que firmen para asegurarse de que ninguna esté bajo una influencia que podría hacerla irrazonablemente crédula o sugestionable. Si hay drogas fiables para la seducción que puedan suministrarse a una víctima potencial sin consentimiento, quizás deberíamos prohibir todo el sexo que no venga precedido por controles de drogas adecuados. Las críticas de las campañas actuales contra definir la violación en las citas tan ampliamente como sea posible podrían argumentar que ya estamos de camino a eso.

No todas las formas de protección dependen de cambios en la ley. La protección más simple contra ser drogado es no beber de un vaso o

recipiente en el que otro haya tenido una oportunidad de meter algo. Llevando la autoprotección un poco más lejos, actualmente existen pruebas químicas simples para la presencia de drogas para la violación en las citas. Discretamente deja caer unas pocas gotas de tu bebida en la tira de la prueba; si cambia de color, recuerda que tienes un asunto urgente en otra parte.[126] Uno puede imaginar versiones más sofisticadas, a medida que la tecnología de defensa mejore para alcanzar a la ofensiva. Quizás acabaremos usando nanotecnología para equiparnos con laboratorios químicos microscópicos que continuamente vigilan nuestra corriente sanguínea y nos hacen saber si hay algo que no debería estar.

Condiciones de empleo

Hasta ahora en la discusión de drogas para el control he estado dando por hecho que se dan a la gente sin su consentimiento. Hay otra forma en que podrían usarse que nos mueve a la frontera entre las drogas que se usan para cambiar mi personalidad y drogas que se usan para controlarme.

Hay muchos trabajos en los que la lealtad es importante. Supón que estoy contratando gente para una empresa cuyos empleados tendrán oportunidades rentables de beneficiarse a costa de la empresa, de apropiarse de pequeños y valiosos objetos o vender los secretos comerciales de la firma a sus competidores. Tras calcular el coste de vigilar a todos todo el tiempo, decido ofrecer dos contratos de trabajo distintos, uno en el que se pague cincuenta mil dólares al año, y otro, cien mil. Solo hay una diferencia entre los dos contratos: el segundo exige que el empleado consuma una droga que le haga leal a la firma.

Se podría objetar que dejar que alguien acceda a un contrato así es como dejarle venderse como esclavo. Se podría responder que prohibir el contrato significa negar el control individual sobre su cuerpo y mente. Y uno podría también puntualizar que lo que he descrito es simplemente una nueva tecnología para un viejo propósito. Firmas,

[126] "Drink Safe Technology" es un paquete de tiras para comprobar el uso de drogas inhibidoras de defensa al ataque sexual.

ejércitos y naciones han estado usando métodos más primitivos para intentar hacer que la gente se sienta leal mucho tiempo.

La droga de la lealtad contractual, sin embargo, plantea algunos asuntos interesantes. Una vez te has tomado la droga, ¿qué va a evitar que el empresario sugiera que voluntariamente le devuelvas la mitad del salario y qué evita que accedas a hacerlo lealmente? Quizás el contrato debería incluir alguna protección especial.

Una cuestión importante aquí es si la droga te hace permanentemente leal, como los padres son permanentemente leales a sus hijos, incluso a los hijos que solo una madre podría amar, o si la lealtad se disipa con la droga. En el último caso, el empresario podría tener que confiar en tu lealtad para hacer que tomes la siguiente dosis, y un empleado leal aun así podría ser distraído. Podría ser más prudente implantar pruebas obligatorias para asegurarse no de que no estás bajo los efectos de las drogas, sino de que lo estás.

LA QUÍMICA DEL AMOR

Las sensaciones de euforia, falta de sueño y pérdida de apetito, así como energía intensa, atención centrada, motivación torrencial y comportamientos orientados hacia la meta por parte del amante, su tendencia de considerar al amado como nuevo y único, y la pasión incrementada frente a la adversidad podrían causarse todas ellas, en parte, por niveles de dopamina y norepinefrina cerebrales por las nubes. Y la reflexión obsesiva del amante acerca del amado podría deberse a niveles cerebrales con un descenso de algún tipo de serotonina.

Helen Fisher, *Por qué amamos: naturaleza y química del amor romántico.*

El patrón de comportamiento que asociamos con enamorarnos lo compartimos con muchas otras especies, un hecho que simplifica mucho la investigación de sus causas y naturaleza; es más fácil conseguir aprobación para experimentos con ratas que con gente. La investigación resultante sobre la relación entre el amor romántico y la

química cerebral proporciona ejemplos posibles de todos los tipos de drogas mentales que he estado discutiendo.

Enamorarse es para alguna gente una experiencia intensamente agradable, y, por supuesto, adictiva, lo que podría explicar por qué algunos hombres se enamoran intensamente de una mujer y luego, cuando sus esfuerzos se ven recompensados con el éxito, pierden el interés y se enamoran de otra. Un ejemplo famoso es Giacomo Casanova, la figura histórica cuyo nombre se ha convertido en un sinónimo de la inconstancia masculina. A juzgar por sus memorias, era una persona mucho más agradable que lo que sugiere el uso moderno de su nombre; parece que realizó esfuerzos considerables para asegurarse del bienestar futuro de sus antiguas amantes, y algunas siguieron siendo sus amigas y se escribieron durante décadas tras el final de la aventura. Pero sí se enamoró de un número considerable de mujeres y la intensidad de su pasión se enfriaba predeciblemente tras un periodo de quizás un mes o dos de su éxito.

Posiblemente, la diferencia entre Casanova y el resto de nosotros solo es una cuestión de cantidad, no de tipo. Amo mucho a mi mujer, pero no estoy enamorado de ella en el mismo sentido en que lo estaba cuando la cortejé por primera vez hace unos treinta años. No solo son diferentes subjetivamente las dos emociones, hay pruebas de que están relacionadas con diferentes neuroquímicos del cerebro. Mis sentimientos de cuando me enamoré de ella eran de alguna forma más como mis sentimientos hacia nuestros hijos, especialmente cuando eran jóvenes, de lo que son mis sentimientos actuales hacia ella. El amor de padre presenta la misma focalización, la misma sensación de que un ser es lo más importante en el mundo, como el amor romántico. Sospecho, pero no lo sé, que con suficiente investigación se podría encontrar que algunos de los mismos neuroquímicos actúan en ambos.

La investigación reciente sobre la naturaleza del amor, centrada en la conexión entre comportamiento y química cerebral, distingue tres comportamientos diferentes, pero relacionados: enamorarse, apego y deseo.[127]

Enamorarse es un patrón de comportamiento familiar por la literatura, películas, televisión y, para la mayoría de nosotros,

---

[127] Fisher, 2004, especialmente el capítulo 4.

experiencia de primera mano. Un síntoma central es la creencia completamente irracional de que una persona es lo más importante en el universo, el centro de la mayoría de los pensamientos, esperanzas y atención. No es un patrón limitado a los humanos: una amplia gama de animales, desde los elefantes hasta las ratas, parecen enamorarse también. En los animales, como en los humanos, el comportamiento está íntimamente relacionado al comportamiento de apareamiento.

Los humanos rara vez siguen enamorados; normalmente, los sentimientos y el comportamiento asociado duran durante meses, no años. A veces el amor viene sucedido por el apego, un patrón de comportamiento asociado con emociones menos intensas y que puede, con suerte, durar una vida. No comprendemos del todo los mecanismos que subyacen en estos patrones de comportamiento, pero parece claro que están asociados con neuroquímicos conocidos y áreas conocidas del cerebro. Supón, como parece probable, que investigaciones ulteriores posibilitan controlar el enamoramiento y desenamoramiento, mantener o destruir las emociones del apego romántico, encender y apagar el amor y el deseo, con una píldora, un parche, una inyección. ¿Qué consecuencias acarreará?

Las consecuencias del uso involuntario son obvias y nada atractivas: una píldora que hace que una hermosa mujer se enamore o, para objetivos a corto plazo, te desee. ¿Y el uso voluntario?

Hace muchos años pasé un vuelo de larga distancia (de Bombay a Sydney) al lado de una mujer del sur de la India, que volaba para reunirse con su marido. Provenía de una sociedad en la que los matrimonios concertados se dan por hecho. Su marido lo habían elegido sus padres para ella, aunque lo había conocido antes de consentir casarse. Yo venía de una sociedad en la que se daba por hecho que los individuos encontraban y elegían a sus propias parejas. Ella aceptaba los arreglos de su sociedad y estaba intrigada por la extraña manera en que hacíamos las cosas; yo sentía lo mismo en la otra dirección. Ella no era una cifra rígida en un texto de historia o antropología, sino un ser humano viviente, obviamente inteligente y reflexivo. Más aún, al menos en nuestro pequeño ejemplo, la superioridad del sistema de Occidente estaba de todo menos claro; ella estaba felizmente casada, yo me acababa de divorciar.

Fue una conversación muy interesante y salí de ella menos seguro de la superioridad de nuestro sistema. La elección de la pareja es, después de todo, una decisión difícil e importante, y es difícil imaginar algo más lejano a un ente fríamente racional que un hombre enamorado. Por otra parte, estar enamorado no es solo una experiencia intensa y conmovedora, es también un preliminar natural y apropiado para una vida de apego, al menos posiblemente diseñado por la evolución para este fin.

Quizás en el feliz mundo de la química moderna uno será capaz de conseguir lo mejor de ambos mundos. Primero selecciono una esposa mediante un análisis apropiadamente tranquilo y objetivo, usando los servicios de un casamentero profesional para encontrar a una mujer hecha idealmente para ser mi mujer, siendo uno de los requerimientos, por supuesto, que yo sea el marido apropiado para ella. Después de que hayamos aceptado el resultado de la búsqueda, justo antes o después de la boda, tomamos nuestras píldoras, nos miramos a los ojos y nos enamoramos profunda y pasionalmente. Tras seis meses o así de dicha extática pero distraída (nuestros jefes están comenzando a preocuparse por nuestra actuación laboral en declive), cambiamos la prescripción de pasión a apego y así cambiamos a un matrimonio largo y satisfactorio. Si en alguna ocasión apropiada futura, como un décimo aniversario, sentimos la necesidad de una segunda luna de miel, quizás todavía queden unas pocas píldoras de la primera prescripción.

Suena a ciencia ficción, pero no está completamente claro que no sea también un hecho muy antiguo que, ojalá, se dé solo en ocasiones. No estoy seguro de si mi amiga india estaba, o había estado, enamorada de su marido, pero ciertamente parecía apegada a él. Es completamente posible que el matrimonio concertado a veces pudiera haber llevado al romance, especialmente en una sociedad en que se segregaba a los jóvenes adultos por sexo, así que podría ser que tu mujer fuera la primera joven apropiada de la que has tenido ocasión de enamorarte.

No solo podría ser el amor una vieja historia, sino también la química. El sexo, como muchos de nosotros hemos observado, tiene concomitantes emocionales. También químicos. «En el orgasmo, los niveles de vasopresina incrementan en los hombres y los de oxitocina,

en mujeres.»[128]Las conexiones entre esas hormona y los neurotransmisores que parecen estar asociados al amor romántico (dopamina, norepinefrina y serotonina) son complicados, pero claramente existen.[129] Es completamente posible que las píldoras que he descrito ya estén construidas dentro de nosotros, al menos de forma débil.

Lo que nos lleva de vuelta a uno de los conflictos centrales de nuestra cultura: la controversia a favor y en contra de la naturaleza. Por rutina utilizamos «natural» como término de alabanza: comida natural, naturaleza sin contaminar, nacimiento natural. Y aun así hemos construido nuestro mundo en gran parte para evitar los defectos de la naturaleza.El nacimiento no natural, hasta e incluyendo la cesárea (actualmente usada en más de un cuarto de todos los nacimientos en EE.UU.) es la razón de que la muerte en el nacimiento sea ahora una tragedia poco común en vez de algo habitual. Muy pocos residentes en Chicago o Houston prefieren, si se les da a elegir, mantener sus casas todo el año a temperatura ambiente. Y casi todos los vegetales que comemos (casi todos cereales, frutas y verduras) no son naturales, sino el resultado de muchas generaciones de cultivo selectivo de plantas naturales que pocos de nosotros consideraríamos que merece la pena comer.

Si no lo queremos en nuestras casas, ¿y en nuestros corazones? ¿Naturaleza o arte? ¿Estamos mejor dejándonos enamorar y desenamorar, metiéndonos y saliendo de camas ocupadas, casándonos y divorciándonos por los procesos naturales maquinados en nuestras mentes y cuerpos, o estamos mejor decidiendo cuándo y a quién amamos por medio de nuestra razón, ayudados por consejo experto cuando sea apropiado, y luego implementando nuestras decisiones mediante las maravillas de la química moderna?

Y, para descender por un momento de tan altas especulaciones, ¿será en el futuro «Se negó a tomar su píldora para el apego» causa legítima para el divorcio? ¿Se convertirá el sexo por diversión en amor por diversión? ¿Ofrecerán los bares para solteros dos bebidas especiales de

---

[128] Fisher, 2004, p. 89.
[129] Fisher, 2004, pp. 89–92.

más, una con una droga para enamorarse, para tomar antes de ir a su casa o a la tuya, y una con el antídoto?

UNA NOTA FINAL

Algunos lectores, siguiendo mis notas del final, podrían haber notado repetidas referencias a obras de Matt Ridley que tratan no solo de drogas, sino de genética. No es por accidente. Los mecanismos químicos que generan nuestras drogas naturales para la mente se encuentran bajo control genético. El estudio de cómo afectan los genes al comportamiento se encuentra íntimamente conectado con el estudio de cómo la química de nuestro cerebro afecta al comportamiento. Estudiar las drogas para la mente inyectando química en los cerebros y viendo cómo reaccionan plantea serias dificultades prácticas y éticas. Una alternativa atractiva es observar a gente que, posiblemente por razones genéticas, se comporta de formas distintas y observar su sangre para ver qué hay en ella.

Hay un segundo vínculo entre los dos estudios. Las drogas podrían proporcionar una forma temporal de hacer lo que los genes hacen para bien. Si resulta que incrementar el nivel de serotonina en el cerebro hace más feliz a la gente, una tentadora solución a corto plazo podría ser alimentar a la gente, o inyectarles, con algo que tenga como resultado el incremento de los niveles de serotonina. Si resulta que funciona, una solución para un plazo aún mayor podría ser la manipulación genética para incrementar el nivel que producimos. Quizás incluso podríamos identificar un «gen de la felicidad», algún gen o grupo de genes que sean comunes en la gente feliz en un grado impactante, y encontrar alguna forma de incrementar artificialmente su frecuencia en la población. Quizás la próxima vez que me encuentre con mi amiga que brilla en la oscuridad debería pedirle una muestra de sangre para pasársela a algún investigador ambicioso.

Tú también puedes tener bebés felices.

PARTE 6

LA CIENCIA FICCIÓN REAL

DIECISIETE

LA ÚLTIMA ENFERMEDAD LETAL

Durante los últimos quinientos años, la duración media de una vida humana en el mundo desarrollado ha llegado a más que duplicarse, mientras que el máximo ha seguido esencialmente igual. Hemos eliminado o reducido enormemente la mayoría de las causas tradicionales de mortalidad, incluyendo asesinos masivos como la viruela, sarampión, gripe y complicaciones del nacimiento. Pero la vejez sigue incurable y siempre letal.

¿Por qué? Frente a él, el envejecimiento parece un diseño pobre. Hemos sido seleccionados por la evolución para el éxito reproductivo; cuanto más vives sin envejecer seriamente, más puedes seguir produciendo bebés. Incluso si ya no eres fértil, seguir vivo y saludable te permite ayudar a proteger y alimentar a tus descendientes.[130]

La respuesta obvia es que si nadie envejeciera y muriera, no habría sitio para que vivieran nuestros descendientes y no quedaría nada para que comieran. Pero esto confunde el interés individual con el grupal; aunque la selección grupal podría haber representado algún papel en la evolución, generalmente se está de acuerdo en que la principal fuerza conductora fue la selección individual. Si sigo vivo, todos mis recursos irán a ayudar a mis descendientes; en tanto que estoy compitiendo por recursos, estoy compitiendo sobre todo con los descendientes de otra gente. Además, evolucionamos en un ambiente en el que aún no nos las habíamos visto con otras causas de mortalidad, así que incluso si la gente no envejeciera, seguirían muriendo, y como media casi tan jóvenes. En las sociedades tradicionales, solo una minoría vivía lo bastante como para que importara envejecer.

Una segunda respuesta posible es que la inmortalidad sería útil, por supuesto, pero no hay forma de producirla. Con el tiempo, nuestros cuerpos se desgastan, la mutación aleatoria corrompe nuestros genes,

---

[130] Para una intrigante representación ficticia de una especie en que los viejos ya no son fértiles, pero se dedican al bienestar de sus descendientes, véase Niven, 1973, y otros libros suyos ambientados en el mismo universo.

hasta que al final el último programa está demasiado dañado para seguir produciendo células que reemplacen a las que han muerto. Esta respuesta tampoco puede ser cierta. Un ser humano es, genéticamente hablando, masivamente redundante: cada célula de mi cuerpo contiene las mismas instrucciones. Es como si fuera una biblioteca con billones de copias del mismo libro. Si algunas de ellas tienen errores de impresión o les faltan páginas, siempre podría reconstruir el texto a partir de otras. Si dos volúmenes no concuerdan, comprueba un tercero, un cuarto, un millonésimo.[131] Además, hay organismos que son inmortales. Las amebas se reproducen por división: donde había una ameba, ahora hay dos. No existe una ameba joven.

Se han propuesto una variedad de explicaciones más plausibles para el envejecimiento. Una que encuentro persuasiva comienza con la observación de que, mientras que las células de mi cuerpo son masivamente redundantes, la única fertilizada de la que crecí no lo era. Un error en esa célula acabó en cada célula de mi cuerpo adulto.

Supón que una de esas mutaciones tenía el efecto de matar al individuo y que se lleva a cabo antes de que sea lo bastante mayor para reproducirse. Obviamente, esa mutación se desvanecería en la primera generación. Supón en lugar de ello que matara a su portador, como media, a los treinta. Ahora la mutación desaparecería hasta cierto punto mediante la selección, pero algunos de mis hijos, quizás incluso algunos de mis nietos, todavía podrían heredarla.

Piensa ahora en una mutación que mata a la edad de sesenta años, en un mundo en que el envejecimiento todavía no existe, pero la muerte por nacimiento, rubeola y tigres de dientes de sable sí, con el resultado de que casi nadie llega a los sesenta. La posesión de esa mutación solo es una desventaja reproductiva muy ligera, así que se filtra solo de forma muy lenta. Siguiendo esta línea de argumentación, cabría esperar que las mutaciones letales que actúen tarde en la vida se acumulen, y que fueran apareciendo nuevas a medida que se fueran eliminando gradualmente las viejas. El proceso se refuerza a sí mismo. Una vez sean comunes las mutaciones que te matan a los sesenta, las que te matan a los setenta no importan mucho: solo puedes morir una vez. El

[131] No sé quién fue el primero en afirmar esto, pero se remonta al menos a Drexler, 1987.

envejecimiento podría ser simplemente la labor de una gran colección de genes letales acumulados que actúan tarde.

Una versión ligeramente diferente de esta explicación comienza con la observación de que en el diseño de un organismo (o cualquier otra cosa) hay costes. Podemos dar a los coches un kilometraje de gasolina mejor haciéndolos más ligeros, al precio de hacerlo más vulnerables al daño. Podemos construir coches que sea invulnerables a cualquier cosa que no sean explosivos de alta intensidad (los llamamos tanques), pero sus cifras de kilometraje no son impresionantes.

Deben de existir precios similares en nuestro diseño. Supón que hay alguna característica de diseño, codificada en los genes, que pueda proporcionar beneficios en la probabilidad de supervivencia o fertilidad a una edad temprana al coste de causar un desmoronamiento incrementado tras los sesenta. A menos que los beneficios sean diminutos en relación a los costes, el efecto neto será un éxito evolutivo incrementado, ya que la mayoría de la gente del ambiente en que evolucionamos no llegaba a los sesenta de todas formas. Así que la evolución elegirá una característica así. Haciendo más general el argumento, las ventajas evolutivas para aumentar el lapso de vida humana máxima eran pequeñas en el ambiente en que evolucionamos, ya que en ese ambiente muy poca gente vivía lo bastante como para morir de vieja. Así que no es sorprendente si los costes a corto plazo superaban los beneficios a largo plazo. Mis genes han realizado los cálculos correctos al diseñarme para el éxito evolutivo en el ambiente de hace cincuenta mil años, pero yo, viviendo ahora y con objetivos que van más allá del éxito reproductivo, preferiría que no los hubieran hecho.

Una razón para entender por qué envejecemos es para hacer algo al respecto, un tema del que me preocupo cada vez más a medida que van pasando los años. Si hay un simple defecto en nuestro diseño, si envejecer se debe a telómeros que van encogiendo o a una falta de vitamina Z, una vez descubramos el defecto podríamos ser capaces de arreglarlo. Si el envejecimiento es el efecto combinado de mil defectos, el problema será más difícil. Pero incluso en ese caso, podría haber

soluciones, o la solución lenta de identificar y arreglar los mil[132] o una solución rápida como una máquina microscópica de reparación de células que pueda entrar en el cuerpo arreglando el daño que las mil causas han producido.

Mi propia suposición es que el problema del envejecimiento se solucionará, aunque no necesariamente a tiempo para que me sirva de algo. Esa suposición está basada en dos observaciones. La primera es que nuestro conocimiento de la biología ha crecido en una tasa enorme en el último siglo o así y sigue haciéndolo. Así que si el problema no es irresoluble por alguna razón (no puedo pensar en ninguna razón plausible por lo que debería serlo), parece probable que el progreso científico durante el próximo siglo haga posible una solución. La segunda es que solucionar el problema es de una importancia enorme y vital para los ancianos, y los ancianos controlan recursos muy abundantes, tanto económicos como políticos.

Si tengo razón, una implicación es que el coste de retardar un poco el envejecimiento podría ser grande, puesto que podría acabar en que yo sobreviva lo bastante para beneficiarme de avances más sustanciales. Actualmente hay una variedad de cosas que uno puede hacer para las que hay alguna razón para creer que retardarán el envejecimiento. Solo es «alguna razón» porque el efecto combinado de la larga vida humana y la dificultad de preparar experimentos con seres humanos significan que nuestra información sobre el tema es muy imperfecta. La mayor parte de la información relevante consiste en la observación de que hacer cosas particulares a ciertas razas de ratones o moscas de la fruta, sujetos experimentales con generaciones cortas y sin derechos legales, obtiene como resultado incrementos sustanciales en la longitud de su vida.

Así, por ejemplo, resulta que las moscas de la fruta transgénicas a las que se les ha proporcionado un gen humano en particular tienen una esperanza de vida más de un 40% mayor que los que no tienen el gen extra. Modificar la dieta en algunas cepas de ratones (proporcionándoles, por ejemplo, un elevado nivel de vitaminas antioxidantes) puede tener efectos similares. Cuando estaba

---

132 Para un proyecto actual que sigue estas líneas, el SENS de DeGrey, véase http://sens.org/.

investigando los argumentos a favor y contra consumir muchos antioxidantes, obtuve una prueba persuasiva de un artículo en la revista *Consumer Reports*.[133] Citaba a un investigador en el campo, que decía que tomar suplementos antioxidantes estaba «basándose en un mecanismo de envejecimiento que no se ha probado», pero añadió que «como varios científicos con los que hemos contactado, se toma un régimen de suplemento que incluye vitaminas C y E, beta-caroteno y una tableta multivitamínica». Como economista, creo que lo que la gente hace es frecuentemente una prueba mejor que lo que dicen.

Una de las formas más efectivas de aumentar la duración de la vida de los ratones resulta ser la privación calórica: se les alimenta con una dieta con el mínimo de calorías necesarias para seguir con vida, pero, por otra parte, adecuada en nutrientes. El resultado es producir ratones con esperanzas de vida muy largas. Si funcionará con los humanos, aún no se sabe, o, una pregunta con interés más inmediato para alguno de nosotros, si funcionaría en humanos que solo comenzaron tarde en la vida. Un padre que eligiera casi matar de hambre a sus hijos se arriesgaría a que se le juzgara culpable de maltrato, pero podría argumentar, basándose en pruebas existentes, que de hecho era el único padre que no lo era.

¿EL INCONVENIENTE DE LA INMORTALIDAD?

Supón que mi suposición es correcta; en algún punto del futuro no muy lejano, con suerte en algún punto de mi futuro, encontramos la cura para el envejecimiento. ¿Cuáles son las consecuencias? A nivel individual son grandes y positivas: una de las peores características de la vida humana se ha desvanecido. La gente que prefiere la mortalidad todavía puede vivir. Los que tienen asuntos sin terminar pueden seguir con ellos.

Pero mientras que estoy completamente a favor de parar mi envejecimiento, no se sigue de ello que esté a favor de parar el tuyo.

---

[133] *Consumer Reports*, January, 1992, p. 12. Sin embargo, algunos estudios más recientes no han conseguido detectar ningún beneficio de los suplementos antioxidantes, y la cuestión todavía se encuentra abierta.

Una razón para no estarlo es la preocupación acerca del crecimiento de la población. Resulta que no comparto esa preocupación, al haber llegado a la conclusión hace mucho de que, en todo lo cercano a los niveles de población actuales, el mero número de gente no es un problema serio.[134] Esa conclusión se reforzó durante los años cuando los predicadores líderes de la condena de la población procedieron a acumular una serie de profecías fallidas sin igual fuera de las sectas religiosas enloquecidas. Los lectores que discrepen, como muchos hacen, podrían querer echar un vistazo a las obras del fallecido Julian Simon, posiblemente la crítica más capaz y ciertamente la más enérgica contra la tesis de que el aumento de la población lleva a la catástrofe. Prefiero pasar a temas que considero más interesantes.

«Senador» significa «anciano»

Una monarquía absoluta es una en la que el soberano hace lo que quiere siempre que agrade a los asesinos.

Ambrose Bierce, *El diccionario del diablo*

Uno es el problema de la gerontocracia, el gobierno de los ancianos. Con nuestro sistema político, los titulares tienen una ventaja enorme: en el Congreso casi siempre consiguen la reelección.[135] Si el envejecimiento para y no cambia nada más, nuestros representantes envejecerán de forma constante. Un titular al que se le garantiza la

---

[134] Supón que todos viven para siempre; ¿a qué velocidad crece la población? Empezando con lo que era una población estable de diez mil millones, si cada pareja tiene dos hijos y luego para, obtenemos unos quince mil millones en treinta años, veinticinco mil millones en un siglo; el patrón de crecimiento acaba siendo linear. Por otra parte, si cada pareja tiene dos hijos cada cuarenta años, acabamos con un patrón de crecimiento exponencial del 2,5% anual, lo que proporciona veintiún mil millones en treinta años, ciento dieciocho mil en un siglo, y más de un billón en dos siglos.

[135] Supón que todos viven para siempre; ¿a qué velocidad crece la población? Empezando con lo que era una población estable de diez mil millones, si cada pareja tiene dos hijos y luego para, obtenemos unos quince mil millones en treinta años, veinticinco mil millones en un siglo; el patrón de crecimiento acaba siendo linear. Por otra parte, si cada pareja tiene dos hijos cada cuarenta años, acabamos con un patrón de crecimiento exponencial del 2,5% anual, lo que proporciona veintiún mil millones en treinta años, ciento dieciocho mil en un siglo, y más de un billón en dos siglos.

reelección es libre de hacer lo que quiera dentro de lo que cabe. Así que un resultado sería debilitar aún más el control democrático sobre los gobiernos democráticos. Otro podría ser crear sociedades dominadas por ancianos: mandonas, cautelosas, conservadoras.

El efecto sobre los sistemas no democráticos podría ser incluso peor. En un mundo sin envejecimiento parece probable que Salazar todavía estaría gobernando Portugal y Franco, España. Habría sido Stalin, equipado con un arsenal de misiles termonucleares, quien habría presidido, y se habría esforzado al máximo para evitar, la desintegración final de la Unión Soviética. Una vez solucionado el problema del envejecimiento, el dictador se volvería una condición permanente. Siempre que, por supuesto, ese dictador tomara las suficientes precauciones contra otras fuentes de mortalidad.

El problema no se limita al mundo de la política. Se ha argumentado que el progreso científico consiste en que los jóvenes científicos adopten nuevas ideas y los científicos viejos se mueran. Es aterrador imaginar las universidades que nuestro sistema de ejercicio académico podría producir sin jubilación obligatoria, ahora ilegal en EE.UU., o sin mortalidad.

En algunas de estas preocupaciones se encuentra implícito un supuesto enterrado: que estamos curando los efectos físicos del envejecimiento, pero no los mentales. Si ese supuesto es razonable depende de por qué los ancianos piensan de forma distinta a los jóvenes. Una respuesta, popular entre los ancianos, es que saben más. Si es así, quizás la gerontocracia no es tan mala. Otra es que el cerebro tiene capacidad limitada.[136] Habiendo aprendido un sistema de ideas, podría no haber sitio para poner otro, especialmente si son incoherentes entre sí. Los humanos, viejos y jóvenes, demuestran una fuerte preferencia por las creencias que ya tienen; los ancianos tienen más creencias.

Una forma de comprender el envejecimiento es como un cambio de inteligencia fluida a cristalizada. La fluida es lo que se utiliza para

---

[136] Quizás fue Sherlock Holmes quien lo afirmó de forma más famosa: «Un hombre debería mantener su pequeño cerebro guardado con todos los muebles que sea probable que necesite, y el resto puede ponerlo en el trastero de su biblioteca, donde puede cogerlo si lo necesita.» http://www.quoteworld.org/author.php?thetext=Sir%20Arthur%20Conan%20Doyle.

resolver un problema nuevo. La cristalizada consiste en recordar la solución que encontraste la última vez y usarla. Cuanto mayor eres, más problemas has resuelto ya y menos coste futuro hay de encontrar soluciones nuevas y posiblemente mejores. Este argumento me vino de una forma impactante hace algunos años cuando observé a un octogenario muy inteligente ignorando la evidencia de lo que resultó ser un fuego que se aproximaba (olor a humo, información de otros que lo habían visto) hasta que vio las llamas con sus propios ojos.

Es posible, por supuesto, que si acabáramos con el envejecimiento (mejor aún, hiciéramos posible revertir sus efectos), el resultado sería gente anciana con las mentes de los jóvenes. También es posible que descubriéramos que las características mentales de los ancianos, los que no están seniles, eran una consecuencia no de deterioro biológico, sino de sobrecarga de información, la respuesta de una mente limitada a demasiada acumulación de experiencia.

Suficiente mundo y tiempo

Cuando contemplamos la posibilidad de vivir unos cuantos siglos de más, una pregunta obvia es qué hacer con ellos. Habiendo criado una familia, envejecido, y luego habiendo recuperado mi juventud, ¿decidiría ver si puedo hacerlo todavía mejor una segunda vez o llegaría a la conclusión de que eso era algo que ya había hecho? Una débil prueba para la primera alternativa viene proporcionada por el patrón nada común de abuelos criando a sus nietos cuando los padres del niño demuestran ser incapaces o no están dispuestos a realizar la tarea.

La misma pregunta surge en otros contextos. Habiendo tenido una carrera como economista, ¿continuaría la línea de mi trabajo pasado o decidiría que esta vez quería ser novelista, empresario, explorador del ártico? Es una observación familiar que, en muchos campos, los académicos hacen su mejor trabajo y el más original cuando son jóvenes. Una vez mi padre sugirió el proyecto de financiar a académicos de éxito que ya no sean tan jóvenes para volver a formarse en un campo completamente distinto, para ver si el resultado era un segundo estallido de creatividad. En un mundo sin envejecimiento, ese patrón

podría volverse mucho más común. Y un novelista o empresario que primero había sido un economista académico o un oficial de la marina podrían aportar una formación interesante a su nueva profesión.[137]

Una alternativa es el ocio. No podemos jubilarnos todos, ya que tiene que quedar alguien para cortar el césped, cultivar la comida y hacer el resto del trabajo del mundo. Pero podría ser posible que la mayoría de nosotros nos jubiláramos o que todos nos jubiláramos casi por completo. El capital, como la mano de obra, es productivo: más maquinaria y mejor, otras formas de producción mejorada, permiten que una persona haga el trabajo de diez o cien. Piensa en la impactante caída en la fracción de la fuerza productiva estadounidense inmersa en la producción de comida, de casi todo el mundo a casi nadie en el espacio de un siglo.

Lo productivo que es el capital en el presente lo muestra la tasa de interés, el precio que la gente está dispuesta a pagar por usar el capital. La tasa de interés real, la tasa tras tener en cuenta la inflación, ha sido generalmente del 2%. Si ese patrón se mantiene en el futuro, podrías pasar los primeros cincuenta años de edad adulta gastando (digamos) ochenta mil dólares al año, gastando cincuenta mil dólares, ahorrando el resto, acumula unos 2,54 millones de dólares y luego pasa el resto de tu larga vida viviendo del interés: cincuenta mil ochocientos dólares al año por comida, vivienda y una buena conexión a Internet. Podrías, si lo desearas, seguir trabajando a tiempo parcial, escogiendo esas actividades que te gustaba hacer y que otra gente esté dispuesta a pagar.[138] Un buen trabajo, si puedes conseguirlo. Uno puede imaginarse fácilmente un futuro que siguiera estas líneas de que una gran fracción de la población, incluso una gran mayoría, estuviera al menos retirada en parte.

---

[137] Elizabeth Moon fue teniente primera de los marines estadounidenses antes de retirarse a escribir ciencia ficción y fantasía. Para un ejemplo más famoso, piensa en Joseph Conrad, primero marinero y luego novelista.

[138] Esta discusión ignora toda una variedad de complicaciones, como el efecto de tal patrón de ahorro y consumo sobre la tasa de interés de mercado, que nos llevaría más allá de los límites de este libro. Véase el intrigante ensayo de Robin Hanson en http://www.primitivism.com/uploads-dawn.htm.

Mientras piensas en cómo pasar tu segundo siglo, podrías querer considerar las consecuencias sociales de eliminar los marcadores de edad. En un mundo en que envejecer se encuentra completamente bajo tu control, una joven mujer de veinte años podría salir con un joven cien años mayor que ella, y él podría o no decírselo. Lo mismo sucede ya en la red, donde una ligona de doce años podría ser casi cualquier cosa, incluyendo un agente masculino del FBI de cuarenta años. Si tú, un abuelo con una pensión de jubilación y un siglo tras de ti, pudieras volver a la universidad como estudiante de primer año, ¿lo harías? ¿A tiempo completo? Muchas chicas monas. Las mujeres de tu propia generación son igual de monas, gracias a la misma biotecnología avanzaba que hace que tengas dieciocho de nuevo, pero lo de verdad tiene sus encantos. Quizás.

Vida o cien años, lo que sea más corto

La inmortalidad también plantea asuntos para nuestro sistema legal. Piensa en un delincuente sentenciado de por vida. ¿Lo interpretamos como «lo que solía ser una sentencia de por vida», digamos, hasta los cien años? ¿O literalmente?

Para responder esa pregunta, comenzamos preguntando por qué encerraríamos a alguien de por vida en primer lugar. Hay al menos dos respuestas plausibles, asociadas con dos teorías diferentes del castigo penal. Una es que encerramos a un asesino por la misma razón que encerramos a un tigre: es peligroso para los demás, así que queremos mantenerlo donde no pueda hacer mucho daño. Esa es la teoría del castigo penal a veces descrita como *incapacitación*. La otra es que encerramos a un asesino para imponerle un precio, uno lo bastante alto para que otra gente que contemple la posibilidad de cometer un asesinato elija no incurrir en él. Esa es la teoría descrita como *disuasión*. En la práctica, por supuesto, podemos operar según ambas teorías a la vez, creyendo que se puede disuadir a algunos delincuentes, a otros solo incapacitarlos, y que no siempre podemos estar seguro de con cuál se puede hacer cuál.

Si nuestro objetivo es la disuasión, siglos de encarcelación podría ser una exageración, lo que es un argumento para acabar liberando al convicto. Por otra parte, si nuestro objetivo es la incapacitación, podríamos querer mantenerle dentro. Bajo las actuales circunstancias, es improbable que un asesino de noventa y nueve años represente mucho peligro para alguien que no sea él mismo, pero si vencemos el envejecimiento, ya podría no ser ese el caso.

Una tercera justificación del encarcelamiento es la rehabilitación, cambiar a los delincuentes para que ya no quieran cometer delitos. Esa es la teoría que nos proporcionó «reformatorios» para reformar a la gente y «penitenciarías» para que la gente se arrepienta. Es difícil ver por qué, según esa teoría, tendríamos condenas de por vida; quizás uno podría argumentar que hay alguna gente a la que le cuesta más tiempo rehabilitarse que el que probablemente vayan a durar. Si es así, uno podría reinterpretar «vida» como «hasta los cien años o hasta la rehabilitación, lo que sea más largo».[139]

Hasta ahora, en este capítulo he estado considerando las consecuencias de soluciones hipotéticas para el problema del envejecimiento. Ahora pasamos a uno que ya está aquí.

UN SIGLO FRÍO EN EL INFIERNO

Así, las pruebas clínicas apropiadas serían:

1. Selecciona N sujetos.
2. Presérvalos.
3. Espera cien años.
4. Mira si la tecnología del 2100 puede revivirlos.

El lector podría darse cuenta de un problema: ¿qué decimos al paciente enfermo terminal antes de que se completen las pruebas?

Ralph Merkle, de una defensa de la criónica en línea.

---

[139] Posiblemente, la «rehabilitación» podría haberse vuelto mucho más fácil como resultado de otras tecnologías: la inmersión en realidad virtual para mostrar al criminal cómo se veía el crimen desde el punto de vista de la víctima o el uso de biología avanzada o nanotecnología para corregir la personalidad del criminal. Ambas plantean la posibilidad de otros usos menos justificables.

La idea de la suspensión criónica (mantener congelada a la gente con la esperanza de algún día deshelarla, revivirla y curar lo que la mató) ha estado en el aire desde hace algún tiempo. Los críticos lo ven como un fraude o una ilusión, y comparan el problema de deshacer el daño que los cristales de hielo han hecho a las células durante el proceso de congelación con convertir una hamburguesa de nuevo en una vaca viva.[140] Los que apoyan la idea afirman que a medida que mejora la tecnología de congelar órganos vamos aprendiendo a cómo disminuir el daño (entre otras cosas, reemplazando el agua del cuerpo por el equivalente en anticongelante durante el proceso de congelación). Nadie ha convertido un riñón de un ratón en una hamburguesa y la ha reconvertido en un riñón que funcione, pero aparentemente el equivalente sí se ha realizado exitosamente (una vez) con la congelación. Y argumentan que a medida que mejore la tecnología necesaria para revivir un cuerpo congelado (en última instancia, quizás, mediante el desarrollo de nanotecnología capaz de hacer reparaciones a nivel celular), se volverá más sencillo deshacer el daño que no podemos evitar. Por último y más convincentemente, afirman que sean cuales fueres tus posibilidades de que te hagan regresar de entre los muertos si congelas tu cuerpo, apenas pueden ser peores que las posibilidades si te dejan pudrirte.[141]

Supón que aceptamos sus argumentos hasta el punto de considerar la resurrección como al menos una posibilidad. Entonces nos enfrentamos con una variedad de problemas interesantes, legales y sociales. La mayoría se reducen a una simple pregunta: ¿cuál es el estatus de un cadáver criogenizado? ¿Es un cadáver, una persona viva incapaz de actuar temporalmente, u otra cosa? Si estoy congelado, ¿mi mujer es

---

[140] «Creer que la criónica podría reanimar a alguien que ha sido congelado es como creer que puedes convertir una hamburguesa de nuevo en una vaca». (El criobiólogo Arthur Rowe, citado en «Frozen Future», *National Review*, 9 de julio del 2002. Una sección de preguntas más frecuentes de una web señala en respuesta a esto que hay algunos vertebrados que pueden sobrevivir al congelamiento, pero que ninguno puede sobrevivir a la pulverización: http://www.faqs.org/faqs/cryonics-faq/part4/. Los procedimientos actuales para la suspensión criónica intentan minimizar el daño de los cristales de hielo reemplazando los fluidos corporales por lo que es, en efecto, anticongelante. Un paso más allá, disponible actualmente para la suspensión de solo la cabeza, es vitrificar en vez de congelar el agua corporal, con lo que la vuelven sólida sin dejar que cristalice.

[141] Para una discusión inteligente de un defensor de la criónica, véase http://www.merkle.com/cryo/.

libre de volver a casarse? Si me descongelan, ¿con cuál de los dos está casada? ¿Heredan mis descendientes, y, si es así, puedo reclamar mi propiedad cuando me reúna con los vivos?

Muchos de estos son asuntos que pueden tratarse (si la suspensión se vuelve común, se tratarán) mediante acuerdos privados. Si la ley considera a mi mujer como viuda, todavía puede elegir considerarse esposa; si la ley me considera congelado pero vivo, puede pedir un divorcio. No estoy en posición para reaccionar. Si estoy preocupado por quedarme con mi riqueza para sustentarme en la segunda parte de mi vida, hay instituciones legales, fideocomisarios y similares que proporcionan a los muertos cierto grado de control sobre sus activos.

Esas instituciones no son perfectas (podría revivírseme en cien años para descubrir que un fideocomisario ha robado mis ahorros, o Hacienda, o la inflación, pero podrían ser lo mejor a lo que podemos aspirar). Su principal limitación es una que se aplica a casi todas las soluciones, el hecho de que durante un periodo de un siglo o más, las instituciones legales y sociales podrían cambiar de formas que vencen incluso los intentos prudentes de planificación para el momento de resucitar. Una alternativa es transferir riqueza de formas que no dependan de instituciones estables, quizás enterrando una colección de objetos valiosos en algún sitio y preservar su localización solo en la memoria. Esa táctica también plantea riesgos: podrías revivir, cavar tu tesoro y descubrir que las monedas de oro y sellos únicos ya no valen mucho. Si lo hubieras sabido, habrías enterrado las diez primeras ediciones de este libro.

Otros problemas tienen que ver con adaptar las normas legales a un mundo en que un número sustancial de gente no está del todo viva ni del todo muerta. Si cometes un delito y se te congela, ¿sigue funcionando la prescripción, proporcionándoseme una tarjeta para salir de la cárcel si sigo congelado lo bastante? Si se me ha condenado a cincuenta años en la cárcel y, tras diez de ellos, «muero» y se me congela, ¿sigue corriendo mi sentencia? ¿Y una sentencia de por vida?

Un problema más inmediato es el de alguien que quiere congelarse un poco antes de morir en vez de un poco después. Si la congelación hace imposible revivirme, morir seguramente lo haga más difícil. Y algunas

enfermedades (el cáncer es un ejemplo obvio) hacen un daño masivo mucho antes de la muerte real. Una vez parece que la muerte es cierta, hay muchos motivos a favor de congelarse primero. Por el momento, sin embargo, no es una opción legal. La ley contra el suicidio no se puede ejecutar contra la persona a la que afecta más directamente (al menos, no hasta que reviva, momento en el que retroactivamente deja de ser suicidio), pero se puede ejecutar contra la gente que lo ayudó. Bajo la ley actual, congelar a alguien antes de la muerte, incluso diez minutos antes, es asesinato.

La forma más simple de cambiar eso es interpretar la congelación no como muerte, sino como un procedimiento médico de riesgo cuyo resultado no se conocerá durante algún tiempo. Es legal y ético que un cirujano realice una operación que podría matarme si las posibilidades sin el procedimiento son incluso peores. La probabilidad de resurrección no tiene que ser muy alta para cumplir ese requisito si la alternativa es morir. Si no, uno podría cambiar la ley, como ha hecho un estado federado, para legalizar el suicidio con ayuda.

DIECIOCHO

LEGOS MUY PEQUEÑOS

Los principios de la física, que yo vea, no hablan contra la posibilidad de maniobrar cosas átomo por átomo. No es un intento de violar ninguna ley; es algo, en principio, que se puede hacer; pero en la práctica nunca se ha hecho porque somos demasiado grandes.

Richard Feynman, «Hay bastante espacio al fondo», charla pronunciada en 1959.[142]

Todos sabemos que los átomos son pequeños. El número de Avogadro describe lo pequeños que son. Escrito por completo es algo así como 602 400 000 000 000 000 000 000. Esta es la relación entre los gramos, la unidades usadas para medir la masa de los objetos (una moneda de diez centavos pesa poco más de dos gramos) y las unidades con las que medimos la masa de los átomos. Un átomo de hidrógeno tiene un peso atómico de alrededor de un gramo, así que el número de Avogadro es el número de átomos en un gramo de hidrógeno.

Viendo todos esos ceros, puedes ver que incluso objetos muy pequeños tienen muchos átomos. Un pelo humano, por ejemplo, contiene más de un millón de miles de millones. Los transistores microscópicos de un chip informático son pequeños comparados con nosotros, pero grandes comparados con un átomo. Todo lo que construyen los humanos, con excepción de algunos experimentos muy recientes, se construyen a partir de conglomeraciones enormes de átomos.

Nosotros mismos, por otra parte, como todos los entes vivientes, estamos construidos a escala atómica. La maquinaria celular que nos hace funcionar depende de moléculas simples (encimas, proteínas, ADN, ARN y similares), cada una de ellas una complicada estructura de átomos, cada uno en el lugar correcto. Cuando un átomo de una hebra de ADN se encuentra en el lugar incorrecto, el resultado es una

142 Feynman, 1960. Las citas posteriores en el capítulo son traducciones de la misma fuente.

mutación.[143] A medida que mejoramos en la manipulación de objetos muy pequeños, comienza a volverse posible que construyamos como estamos construidos, construir máquinas a nivel atómico montando átomos individuales para producir moléculas que realizan tareas. Esa es la idea central de la nanotecnología.[144]

Un atractivo de la idea es que permite construir cosas que no pueden construirse con las tecnologías presentes. Puesto que los enlaces entre los átomos son muy fuertes, debería ser posible construir fibras muy fuertes a partir de moléculas de hebras largas. Debería de ser posible usar el diamante (meramente una configuración particular de átomos de carbono) como material estructural. Incluso podríamos ser capaces de construir ordenadores mecánicos, inspirados por el fallido diseño del siglo XIX de Babbage. Las partes mecánicas se mueven muy lentamente en comparación con el movimiento de electrones en los ordenadores electrónicos. Pero si las partes se encuentran en una escala atómica, no tienen que moverse muy lejos.

En algunos casos, el objetivo es la pequeñez. Una célula humana es lo bastante grande para tener espacio para la multitud de máquinas moleculares que nos hacen funcionar. Con una nanotecnología lo bastante avanzada, debería ser posible añadir una más: una máquina de reparación celular. Imagínatela como un submarino robótico que entra en una célula, arregla lo que está mal y luego sale de esa célula y avanza a la siguiente. Si podemos construir nanocomputadoras mecánicas, podrían ser un submarino robótico muy inteligente.[145]

El cuerpo humano contiene alrededor de cien billones de células, así que arreglar todas ellas con una máquina de reparación celular llevaría un rato. Pero no hay razón para limitarnos a una. O a diez. O a un millón. Lo que nos lleva a otra ventaja de la nanotecnología.

Los átomos de carbono son todos iguales (para ser más precisos, los doce átomos del carbono son todos iguales, pero voy a ignorar las complicaciones introducidas por los isótopos en esta discusión).

---

[143] Esto es quizás decir demasiado, ya que parte del ADN, aparentemente, no lleva información útil.

[144] Los lectores interesados en el tema deberían empezar probablemente por Drexler, 1987. Se encuentra en http://www.foresight.org/EOC/index.html.

[145] Mis agradecimientos a Robert Freitas y Eric Drexler por sus útiles comentarios en este capítulo.

También lo son los de nitrógeno, hidrógeno, hierro. Imagínate a ti mismo, encogido hasta un tamaño pequeño hasta lo imposible, construyendo nanomáquinas. Desde tu punto de vista, el mundo está hecho de partes idénticas intercambiables, como legos diminutos. Elige cuatro hidrógenos idénticos, únelos a un átomo de carbón y tienes una molécula de metano. Repítelo y tienes otra, perfectamente idéntica.

No puedes empequeñecerte tanto, por supuesto, ya que tú mismo estás hecho de átomos y no puedes encogerlos. Así que nuestro primer proyecto, una vez resuelto lo básico de la tecnología, es construir un *ensamblador*. Un ensamblador es una máquina a nanoescala para construir otras máquinas a nanoescala. Piensa en ello como un robot diminuto, donde «diminuto» podría significar construido de poco menos que mil millones de átomos. Es lo bastante pequeño para ser capaz de manipular átomos individuales, montándolos según la forma deseada. Esto no es para nada trivial, ya que los átomos no son en realidad legos y no pueden ser manipulados y juntados de la misma forma. Pero sabemos que es posible montar átomos para formar moléculas; nosotros, y otras criaturas vivientes, lo hacemos por rutina, y algunas de las moléculas que construimos dentro de nosotros son muy complicadas.[146] Los químicos orgánicos, con un control mucho menos detallado sobre el material del que tendría un ensamblador, alcanzaron el éxito en montar de forma deliberada moléculas moderadamente complicadas.

Una vez tengas un ensamblador, escribes un programa para construir otro. Ahora tienes dos. Cada uno construye otro. Cuatro. Tras duplicar diez veces, tienes más de mil ensambladores; tras veinte más, un millón. Ahora escribes un programa para construir una máquina de reparación celular y pones a trabajar a los ensambladores. Una vez tengas algo así como mil millones de máquinas reparadoras de células, las inyectas en tu cuerpo, te sientas y te relajas. Cuando terminen, te sientes como una nueva persona. Y lo eres.[147]

---

[146] Feynman, en su discurso de 1959, discutió creae herramientas de construcción pequeñas para usarlas para construir herramientas más pequeñas, y así sucesivamente. La misma idea aparece en la historia de Robert Heinlein «Waldo» (Heinlein, 1950).

[147] Para una discusión más detallada, véase Freitas (1999, sección 8.5.1), en http://www.nanomedicine.com.

Suena a magia. Pero piensa que cien billones de células comenzaron como una sola y alcanzaron sus números actuales mediante un proceso análogo, pero mucho más complicado.

Un amigo mío (Albert R. Hibbs) sugiere una posibilidad muy interesante para máquinas relativamente pequeñas. Dice que, aunque sea una idea muy salvaje, sería interesante que en cirugía pudieras tragarte al cirujano.

Richard Feynmann.

Una máquina de reparación celular sería una nanotecnología muy complicada, por supuesto; aunque podríamos acabar llegando a ellas, es improbable que suceda muy pronto. Es probable que los materiales extrafuertes, o las drogas médicas diseñadas en un ordenador, átomo a átomo, sean aplicaciones más tempranas de esta tecnología. Para que vayamos tirando mientras esperamos la máquina de reparación de células, Ralph Merkle propuso y Robert Freitas desarrolló más una ingeniosa propuesta para una versión mejorada de un glóbulo rojo: un tanque de aire comprimido a nanoescala.[148] Su ventaja se vuelve clara el día que tienes un ataque al corazón y tu corazón para de latir. En vez de caerte muerto, pide una cita de urgencia con tu doctor, métete en el coche y conduce hasta ahí, funcionando durante varias horas con la reserva de oxígeno que ya se encuentra en tu flujo sanguíneo.

Se podría utilizar la nanotecnología para construir objetos grandes además de pequeños. Se necesitan muchos ensambladores. Pero si comienzas con uno, las instrucciones, en forma de programas que pueda leer e implementar, muchos átomos de todos los tipos necesarios, y un poco de tiempo, podemos producir muchos ensambladores. Con los suficientes y con el *software* para controlarlos, podemos construir casi cualquier cosa. Si la idea de un objeto muy grande construido por maquinaria molecular te parece improbable, piensa en una ballena.

---

148 Para una discusión más detallada, véase Freitas (1999, sección 8.5.1), en http://www.nanomedicine.com.

Verás, los materiales no cuestan nada. Así que quiero construir mil millones de fábricas diminutas, modelos de cada una, que se fabriquen simultáneamente, perforando agujeros, pegando partes, y así sucesivamente.

Richard Feynmann

Como la mayoría de la tecnología nueva y sin probar, la nanotecnología todavía es controvertida, al argumentar algunos autores que la tecnología es y será siempre imposible por una variedad de razones. El contraejemplo más obvio es la vida, una nanotecnología que funciona basada en máquinas moleculares construidas en su mayoría de carbono.

Uno podría suponer que, incluso si la nanotecnología se desarrolla, cualquier cosa realmente buena que pueda producir ya la habrá producido la evolución. Los glóbulos rojos de aire comprimido habrían sido útiles para nosotros y otros entes vivientes hace mucho tiempo, así que si el diseño funciona, ¿por qué no los tenemos ya?

La respuesta es que aunque la evolución sea un poderoso sistema de diseño, tiene algunas limitaciones importantes. Si una mutación aleatoria cambia un organismo de una forma que incremente su éxito reproductivo, esa mutación se extenderá por la población; tras un tiempo, todos la tendrán, y la siguiente puede empezar de ahí. Así que la evolución puede producir grandes mejoras que ocurren a través de una larga serie de pequeños cambios, cada uno una pequeña mejora. Los biólogos evolucionistas han rastreado cómo órganos complicados, como el ojo, se produjeron mediante una larga serie de pequeños cambios.[149]

Pero si una gran mejora no puede producirse de esa forma, si necesitas las veinte mutaciones correctas todas a la vez en el mismo organismo, es improbable que la evolución lo haga. El resultado es que la evolución ha explorado solo una pequeña parte del espacio de diseño, la serie de formas posibles de unir átomos para hacer cosas útiles.

Los seres humanos también diseñan cosas mediante una serie de pequeños pasos. El F111 no salió completo de los cerebros de los hermanos Wright, y el avión que produjeron funcionaba por un motor

---

[149] Dawkins, 1986.

de combustión interna cuyo diseño básico lo habían inventado y mejorado otros. Pero lo que parece un pequeño paso para pensar de forma humana maneras de unir átomos para hacer algo no es necesariamente pequeño desde el punto de vista de un proceso de mutación aleatoria. Por tanto, cabría esperar que los seres humanos, con las herramientas para construir máquinas moleculares, fueran capaces de explorar diferentes partes del espacio de diseño, construir al menos algunas máquinas útiles que la evolución no consiguió construir. Tanques de aire comprimido muy pequeños, por ejemplo.

Los lectores interesados en argumentos a favor y en contra de la viabilidad de la nanotecnología pueden encontrarlos y explorarlos en línea. Para los propósitos de este capítulo voy a dar por hecho que la idea fundamental de construir cosas a escala atómica usando ensambladores a tamaño atómico es viable y sucederá en algún punto en los próximos cien años. Esto nos permite pensar en el mundo que esa tecnología nos proporcionaría.

***SOFTWARE* MUY DURO**

Para construir un coche nanotécnico necesito ensambladores (producidos en números ilimitados por otros ensambladores), materia prima y un programa, una descripción completa de qué átomos van dónde. La materia prima no debería ser un problema. La suciedad es sobre todo aluminio, junto con grandes cantidades de silicio, oxígeno, posiblemente carbono y nitrógeno; el hierro es el cuarto elemento más abundante en la corteza terrestre. Si necesito elementos adicionales que la suciedad no contenga, siempre puedo llenar una pala de esto y aquello. Añade ensambladores programados, agita, y espera que encuentren los átomos necesarios y los dispongan. Cuando han terminado, tengo una tonelada o dos menos de suciedad, una tonelada o dos más de coche. Suena a magia, o al proceso que produce un roble.

He dejado fuera un elemento que hay que añadir: energía. Una bellota contiene especificaciones de diseño y maquinaria para construir un roble, pero necesita luz solar para dar energía al proceso. De forma similar, los ensambladores necesitarán alguna forma de energía. Una

posibilidad obvia es la energía química, desmontar moléculas de alta energía para obtener potencia y átomos. Quizás tendremos que echar un cubo de alcohol o gasolina en nuestra pila de suciedad antes de que comencemos a agitar.

Una vez tengamos la tecnología básica, lo difícil es el diseño; hay muchos átomos en un coche. Por suerte, no tenemos que calcular separadamente la localización de cada uno; una vez hayamos diseñado la primera rueda, las otras se pueden copiar, y lo mismo con muchas otras partes. Tras haber comprendido la estructura atómica de un micrómetro cúbico o algo así de nuestro parabrisas de diamante, podemos duplicarla una y otra vez con el resto. Pero incluso permitiendo la redundancia plausible, diseñar un coche, uno tan bueno como la tecnología te permita construir, va a ser un gran proyecto.

Acabo de describir una tecnología en la que la mayoría del coste de producir un producto es el del diseño inicial. Ya tenemos una tecnología con esas características: el *software*. Producir la primera copia de Microsoft Office llevó una gran inversión de tiempo y esfuerzo por parte de un gran número de programadores. La segunda copia usó un grabador de CD, consumió un disco CDR y costó menos de un dólar. Una implicación de la nanotecnología es una economía para producir coches muy parecida a la economía que actualmente produce programas de procesamiento de textos.

Un problema familiar en la economía del *software* es la piratería. No solo Microsoft puede producir copias adicionales de MS Office por un dólar cada uno: yo también. Ello plantea problemas para Microsoft o cualquier otro que espere recompensa por producir *software* en forma de dinero que se paga para comprarlo.

La nanotecnología plantea el mismo problema, aunque de una manera algo menos severa; no puedo simplemente poner el coche nanotécnico de mi amigo o su ordenador nanotécnico en una disquetera y grabar una copia. Sin embargo, puedo desmontarlo. Para ello, uso nanomáquinas que funcionen como ensambladores, pero al revés. En vez de comenzar con una descripción de dónde van los átomos y ponerlos ahí, comienzan con un objeto (digamos, un automóvil) y quitan los átomos, uno a uno, registrando dónde estaban todos.

Desmontar un automóvil con un desensamblador sería un proyecto tedioso, pero no estoy limitado a uno. Usando mi ejército de ensambladores, construyo un ejército de desensambladores, cada uno equipado con alguna forma de obtener la información que me genera, quizás un radiotransmisor en miniatura, quizás un dispositivo algo menos obvio. Los pongo a todos a trabajar. Cuando han terminado, el coche ha quedado reducido a sus elementos constitutivos y una descripción completa del diseño. Si hubiera ordenadores lo bastante grandes para diseñar el coche, hay ordenadores lo bastante grandes para almacenar el diseño. Ahora programo los ensambladores y me meto en el negocio de los coches.

Una solución para lidiar con el problema de las copias es una antigua tecnología legal, el *copyright*, aplicada a un nuevo tema mediante enmiendas apropiadas a la ley. Habiendo creado mi diseño para el coche, lo protejo con*copyright*. Si te metes en el negocio vendiendo duplicados, te denuncio por violación del *copyright*. Esto debería al menos funcionar un poco mejor en coches que ahora en programas informáticos, porque el primer estadio de la copia (desensamblar, el equivalente a leer un programa de ordenador a partir de un disco) es mucho más difícil en coches, y porque los coches son más grandes y es más difícil ocultarlos que los programas.

La solución podría desmoronarse si, en lugar de vender el coche, el pirata vende el diseño a consumidores individuales, cada uno con su propio ejército de ensambladores listos para trabajar. Ahora hemos vuelto al mundo del*software*. *Software* muy duro. El propietario del *copyright* tiene que ejecutar sus derechos, copia a copia, contra el consumidor definitivo, que es mucho más difícil que ejecutarlos contra alguien que piratea su propiedad al por mayor y la vende.

Supón que, por estas razones u otras, resulta que el *copyright* no realiza el trabajo. ¿De qué otra forma podría pagarse a la gente que diseña estructuras complicadas a nivel molecular por hacerlo? Una posibilidad es las relaciones con otros bienes o servicios que no pueden producirse de forma tan barata (digamos, la tierra). Descargas de un Internet futuro (con un ancho de banda muy amplio) todo el diseño necesario para construir un nuevo coche deportivo, completo, con parabrisas de diamante, un motor que queme casi cualquier cosa y

gaste 3,8 litros por cada 160 km, y un sistema de reconocimiento de patrón radar/óptico combinado que te advierta de cualquier obstáculo en el próximo kilómetro y medio y, si el piloto automático de emergencia está activado, lo evite. Convierte la información en cintas programadas (cintas programadas muy pequeñas) para tus ensambladores, encuentra un punto adecuado del jardín y ponlos a trabajar. La próxima mañana, el coche está ahí, en todo su esplendor.

Entras, giras la llave, aprecias el rugido del motor, pero estás menos contento con otra característica: la voz melódica diciéndote todo lo que no querías saber sobre el adorable desarrollo de casas completado la semana pasada, diseñadas para gente como tú. Tras investigar más, descubres que apagar el anuncio no es una opción. Tampoco lo es deshabilitarlo; el sistema de sonido es una red molecular difundida por la estructura del coche. Si quieres el coche sin el anuncio, tendrás que diseñarlo por ti mismo. Te remontas a los primeros años de Internet, hace treinta o cuarenta años, y a la solución encontrada por los sitios web para el problema de pagar sus facturas.[150]

Otra posibilidad es un coche personalizado. Lo que descargas, esta vez tras pagar por ello, es, sin duda, un coche muy especial, único. Antes de arrancar, comprueba tus huellas dactilares (leídas desde el volante), patrones de retina (escáner por encima del parabrisas) y ADN (nunca echarás en falta unas cuantas células muertas). Si todo concuerda, arranca. El coche está a salvo de ladrones, ya que no pueden arrancarlo. Ni siquiera tienes que llevar una llave; tú eres la llave. Pero si lo desensamblas y creas muchas copias, no serán muy útiles para nadie salvo para ti. Si tu vecino quiere un coche, tendrá que comprar el suyo propio, personalizado para él.[151]

De nuevo, esta es una vieja solución, aunque no muy usada para el *software* del consumidor. Mientras que no tengamos todavía identificación biométrica, el equivalente para los ordenadores es muy

---

[150] Una solución que propuse, en un contexto algo distinto, en Friedman, 1973, capítulo 25.

[151] Un problema con una versión anterior de dicha tecnología, menos el elemento nanotécnico, llamó la atención pública por el Mercedes S-class 2004. Usaba un escáner de huellas dactilares para identificar, lo que llevó a al menos un dueño a perder un dedo por los ladrones de coches: http://www.assaabloyfuturelab.com/FutureLab/Templates/Page2Cols266.aspx.

sencillo; todo cuanto requiere es una CPU con su propio número de serie. Dado este o algún equivalente, algún identificador específico para una máquina en particular, es posible producir un programa que solo arranque en una máquina. Una versión de esta solución usa un *dongle,* un dispositivo que no se copia fácilmente que se adjunta al ordenador y que el programa reconoce.

Una tercera posibilidad para producir diseños nanotécnicos es la fuente abierta: una red de individuos cooperando para producir y mejorar diseños, motivada por alguna combinación de estatus, deseo por el producto final o lo que sea que motivara a los creadores de Linux, Sendmail y Apache.

Como sugieren estos ejemplos, una nanotecnología madura plantea asuntos similares a los del *software*. Esos temas se pueden tratar de formas similares: imperfectas, pero quizás lo bastante bien.

También plantea otros asuntos de una índole distinta y más perturbadora.

EL MARCO HIPOTÉTICO DE LA PLAGA GRIS

Las «plantas» con «hojas» no más eficientes que las células solares de hoy podrían ganar la competición a las plantas reales, llenando la biosfera con un follaje incomestible. Las «bacterias» duras, omnívoras, podrían vencer a las bacterias reales: podrían expandirse como el polen, replicarse rápidamente, y reducir la biosfera a polvo en cuestión de días. Los replicadores peligrosos podrían fácilmente ser demasiado duros, pequeños y de expansión rápida, al menos si no nos preparáramos. Tenemos suficientes problemas controlando virus y moscas de la fruta.

Drexler, *Máquinas de creación*

La vida es buena en conjunto, pero estamos dispuestos a hacer una excepción para ciertas formas de vida, como la viruela. Las máquinas moleculares son, en conjunto, buenas. Pero también ahí podría haber excepciones.

Un ensamblador es una máquina molecular capaz de construir una amplia variedad de máquinas moleculares, incluyendo copias de sí

misma. Debería de ser mucho más sencillo construir una máquina se solo se copie a sí misma: un replicador. Para una prueba del concepto, piensa en un virus, una bacteria o un ser humano, aunque el último no produzca una copia exacta.

Ahora piensa en un replicador diseñado para construir copias de sí mismo, que construye copias, que... Da por hecho que solo usa materiales disponibles al instante en el ambiente natural, con la luz solar como fuente de energía. Cálculos simples sugieren que, en un tiempo increíblemente corto, podría convertir todo en copias de sí mismo a partir de basura, dejando solo los elementos del que haya un exceso de oferta. Eso es lo que ha llegado a conocerse, en los círculos nanotécnicos, como el marco hipotético de la plaga gris.

Si eres el primero que desarrolle una nanotecnología que pueda funcionar, deberían tomarse precauciones. Uno debería evitar, en la medida de lo posible, construir replicadores. Por supuesto, necesitarás ensambladores, y una de las cosas que un ensamblador puede ensamblar es otro ensamblador. Pero al menos puedes asegurarte de que nada más está diseñado para replicar, y un ensamblador, al ser una máquina molecular grande y muy complicada, debería plantear menos amenazas de volverse loco que máquinas más simples cuya única meta de su diseño es la reproducción.

Una precaución que se podría aplicar a los ensambladores, así como a otros replicadores, es diseñarlos para que necesiten algo para funcionar, sea materia o energía, que no se encuentre en el ambiente natural. De esa forma se pueden replicar útilmente bajo tu control, pero no pueden plantear ningún peligro si salen. Otra es darles un periodo de vida limitado, un contador que mantenga un registro de cada generación de copias y desenchufe la máquina cuando alcance su límite preestablecido. Con precauciones como estas para suplementar la obvia de mantener los replicadores en ambientes sellados, podría ser posible asegurarse de que ningún replicador que hayas diseñado para estar a salvo plantee ninguna amenaza seria de convertir el mundo en una plaga gris.

Los replicadores nanotécnicos, como los biológicos naturales, pueden mutar. Un rayo cósmico podría quitar un átomo de la cinta de instrucciones que controle la copia, produciendo copias defectuosas, y

un defecto podría desactivar el límite sobre el número de generaciones. Podría incluso, aunque sea mucho menos probable, eliminar de alguna manera la necesidad del único elemento que no se encuentra disponible en el medio ambiente natural. Liberados de esas constricciones, los replicadores nanotecnológicos salvajes podrían evolucionar gradualmente, como hacen los biológicos. Como replicadores biológicos, su evolución iría hacia el éxito reproductivo incrementado, mejorando más y más en convertir todo lo demás en copias de sí mismos. Y es al menos posible que, explotando posibilidades de diseño visibles para los humanos que diseñaron a sus ancestros, pero inaccesibles para los procesos continuos de la evolución, harían un trabajo mejor que el de los replicadores naturales.

Debería de ser posible diseñar replicadores, si uno es lo bastante astuto, con salvaguardias. Una forma es mediante la redundancia. Podrías, por ejemplo, proporcionar al replicador tres copias de su cinta de instrucciones y diseñarlo para ejecutar una instrucción solo si las tres concuerdan; las posibilidades de que tres rayos cósmicos eliminen el mismo átomo de cada cinta son bajas. Pero bajas no son cero; nuestras células contienen salvaguardias triplemente redundantes contra el crecimiento incontrolado, y aun así tiene lugar el cáncer. Así que uno podría querer asegurarse también de que los elementos no disponibles en el entorno natural representen un papel lo bastante central en el funcionamiento del replicador, de forma que no haya forma plausible de mutar a pesar de la constricción. Tras diseñar el replicador y construirlo, sería deseable ejecutarlo como prueba, usando un ordenador para ejecutarlo a lo largo de muchas generaciones con un número muy grande de cambios posibles para ver si alguno de ellos podría liberar al replicador de los controles que se han diseñado. Si no, podría decidirse que construir replicadores no es, después de todo, tan buena idea.

Casi peor que la enfermedad

He descrito una serie de precauciones que podrían funcionar en un mundo en que solo una organización tiene acceso a las herramientas de

la nanotecnología y esa organización actúa de forma prudente y benevolente. ¿Es eso probable? Frente a ello, un monopolio así parece extraordinariamente improbable en algo como nuestro mundo. Pero quizás no. Supón que se entiende bien la idea de la nanotecnología y un número de organizaciones con recursos sustanciales la aceptan, probablemente los Gobiernos, en un punto anterior a que alguien haya conseguido construir un ensamblador. Cada una de estas organizaciones se enzarza en un extensivo trabajo de diseño informatizado, dando con cómo construir exactamente una variedad de máquinas moleculares útiles una vez tenga los ensambladores para construirlos. Esas máquinas incluyen plagas diseñadoras, drogas de obediencia obtenidas mediante ingeniería, una variedad de superarmamento y muchas más.

Una organización lo consigue: ahora tiene un ensamblador. Muy pronto, tras duplicarse unas cuarenta veces, tiene un billón de ensambladores. Los pone a trabajar construyendo lo que ya ha diseñado. Una semana más tarde, gobierna el mundo. Una de sus primeras acciones es prohibir que otros investiguen sobre la nanotecnología.

Parece un marco hipotético altamente implausible, pero no estoy seguro de que sea imposible; no confío completamente en mi intuición de lo que puede pasar o no con una tecnología de posibilidades tan extraordinarias. El resultado sería un Gobierno mundial con poder casi ilimitado. No veo razón para esperar que se comporte mejor que los Gobiernos pasados con ese poder. Sería una mejora con respecto a la plaga gris, supongo, pero no demasiado mejor.

Si quieres un bosquejo del futuro, imagínate una bota estampada en una cara humana. Para siempre.

George Orwell[152]

[152] Orwell 1949, part III, Capítulo III.

Entre una roca y un lugar duro

Supón que evitamos la dictadura mundial y acabamos, en cambio, con múltiples Gobiernos independientes, algunos de ellos razonablemente libres y democráticos, y con un conocimiento bastante extendido de la nanotecnología. ¿Cuáles son las consecuencias?

Una posibilidad es que todos traten la nanotecnología como un monopolio del Gobierno, que pone a disposición del público los productos, pero no la tecnología. Eric Drexler ha descrito en cierto detalle una versión de esto en la que todo el mundo es libre de experimentar con la tecnología, pero solo en un ambiente (construido nanotecnológicamente) sellado e inaccesible, con la implementación real de los diseños resultantes bajo controles estrictos.[153] Una vez se saque la información básica sobre cómo hacer nanotecnología, la ejecución de estas reglamentaciones podrían depender de que el liderazgo del Gobierno en la carrera de armamento nanotecnológico le provea de dispositivos de vigilancia y control que hagan parecer primitivos los videomosquitos de un capítulo anterior. De nuevo, una perspectiva no muy atractiva, pero una mejora con respecto a que todos nosotros nos convirtamos en una plaga gris.

El problema con esta solución es que se parece mucho al caso de poner al zorro a guardar el gallinero. Los individuos privados podrían investigar ocasionalmente sobre cómo matar gente y destruir cosas, pero la cantidad abrumadora la realizan los Gobiernos para propósitos militares. Las mismas organizaciones que, en esta versión, tienen control sobre el desarrollo y uso de la nanotecnología son los que más probablemente gasten recursos sustanciales encontrando formas de usar la tecnología para hacer lo que la mayoría del resto de nosotros consideramos malas.

Un resultado posible es una plaga gris diseñada deliberadamente como máquina del día del juicio final por parte de un Gobierno que quiere la capacidad para amenazar al resto con un suicidio universal. En un caso menos extremo, podríamos esperar ver mucha investigación sobre el diseño de máquinas moleculares para matar a altas cantidades

---

[153] El Drexler’s Foresight Institute ha propuesto una serie de directrices para evitar alguno de los riesgos de la nanotecnología: http://www.foresight.org/.

de gente (de forma selectiva) o destruir grandes cantidades de propiedad (de otras naciones). Los Gobiernos que realizan investigación militar, si bien prefieren evitar matar a sus propios ciudadanos en el proceso, están dispuestos a asumir riesgos, como sugirieron los incidentes como el del accidente en una instalación de guerra biológica soviética que mató a varios cientos de personas de una ciudad colindante.[154] Y funcionan en una atmósfera de secretismo que podría hacer difícil que otras personas se den cuenta de y señalen riesgos en su trabajo que a ellos no se les habían ocurrido. Hay una posibilidad muy real de que las máquinas moleculares deliberadamente destructivas resulten ser incluso más destructivas de lo que sus diseñadores pretendieron o de que salgan antes de lo que quieran sus diseñadores.

Piensa en dos mundos posibles. En el primero, la nanotecnología es un negocio difícil y caro; se requieren miles de millones de dólares de equipamiento y mano de obra cualificada para hacer cosas útiles. En ese mundo, es improbable que la plaga gris se produzca deliberadamente por mano de nadie salvo de un Gobierno, y cualquier organización lo bastante grande para producirla por accidente probablemente esté lo bastante bien organizada para tomar precauciones. En ese mundo, las defensas contra la plaga gris (de forma más general, las máquinas moleculares diseñadas para proteger a los seres humanos y su propiedad de una amplia variedad de riesgos, incluyendo las máquinas moleculares destructivas, plagas a medida y peligros más mundanos) serán grandes vendedores, y se dedicarán grandes recursos a diseñarlas comercialmente. En ese mundo, hacer de la nanotecnología un monopolio gubernamental hará poco para reducir el riesgo, ya que los Gobiernos serán la principal fuente de ese riesgo, pero podrían reducir sustancialmente las posibilidades de protegernos contra él.

En el segundo mundo, quizás el primero unas pocas décadas más tarde, la nanotecnología es barata. No solo el Departamento de Defensa de EE.UU. puede diseñar una plaga gris si lo desea: también tú puedes diseñarla, en tu escritorio. En este mundo, nada salvo un pequeño número de dictadores que se mantienen en el poder sobre los rivales y

[154] http://www.pbs.org/wgbh/pages/frontline/shows/plague/sverdlovsk/;http://www.nbc-med.org/SiteContent/MedRef/OnlineRef/CaseStudies/cssverdlovsk.html.

súbditos por el liderazgo en la carrera por el armamento nanotécnico va a mantener la tecnología fuera del alcance de quien la quiera. Y no está claro que siquiera eso sea suficiente.

En este segundo mundo, el equivalente nanotécnico a las plagas diseñadas existirá por las mismas razones que existen ahora los virus informáticos. Algunos surgirán de la manera en que lo hizo el gusano de Internet original: el trabajo de alguien muy listo, sin malas intenciones, que crea un error de más. Algunos se diseñarán para sembrar el mal y acabarán haciendo más mal que el que se pretendía. Y unos pocos se crearán deliberadamente como instrumentos apocalípticos por parte de gente a la que por una razón u otra les gusta la idea.

Antes de que llegues a la conclusión de que el fin del mundo se cierne sobre ti, piensa en el otro lado de la tecnología. Con suficientes máquinas reparadoras de células trabajando, las plagas diseñadas podrían no ser un problema. Los seres humanos quieren vivir y pagarán por el privilegio. Los recursos que se invertirán para diseñar protecciones contra las amenazas, nanotécnicas o de otra índole, será mucho mayor que los recursos (privados) que se destinen para crear esas amenazas, como en el presente, en el que disponemos de herramientas mucho más limitadas. A menos que resulte que, con esta tecnología, el ataque tenga una ventaja abrumadora sobre la defensa, las defensas nanotécnicas deberían neutralizar casi por completo la amenaza del terrorista del sótano o el que experimenta sin cuidado. La única amenaza seria vendrá de organizaciones dispuestas y capaces de gastarse miles de millones de dólares creando auténticos asesinos moleculares de primera clase. Casi todas ellas, Gobiernos.

El párrafo anterior contenía una advertencia crucial: que el ataque no sea mucho más sencillo que la defensa. La historia de la plaga gris sugiere que podría serlo, que las máquinas moleculares simples diseñadas para convertir todo el ambiente en copias de sí mismas podrían tener una ventaja abrumadora sobre sus oponentes más elaborados.[155]

---

[155] Para un análisis mucho más detallado del problema de la plaga gris (también conocida como ecofagia), véase Freitas, 2000, en http://www.foresight.org/NanoRev/Ecophagy.html.

Se ha realizado el experimento; los resultados hasta ahora sugieren que ese no es el caso. Vivimos en un mundo poblado por máquinas moleculares. Todas ellas, desde los virus hasta las ballenas azules, se han diseñado con el propósito[156] de convertir lo máximo del medio que puedan en copias de sí mismas. Lo llamamos éxito reproductivo. Hasta ahora, al menos, los simples no han resultado tener una ventaja abrumadora sobre los complicados: las ballenas azules y los seres humanos todavía siguen ahí.

Eso no garantiza la seguridad en un futuro nanotécnico. Como apunté antes, la nanotecnología expande enormemente la región del espacio diseñado que es accesible: los seres humanos serán capaces de crear cosas quela evolución no. Es concebible que, en el espacio expandido de diseños posibles, la plaga gris resulte ser el ganador. Todo cuanto podemos decir es que, hasta ahora, en el espacio más restringido de vida basada en carbono capaz de ser producida por la evolución, no ha resultado así.

Tratando con la nanotecnología, nos enfrentamos a una elección entre soluciones centralizadas (en el límite, un Gobierno mundial con un monopolio nanotécnico) y soluciones descentralizadas. Como norma general, prefiero con mucho la última. Pero una tecnología que plantea la posibilidad de que un adolescente con talento produzca en su sótano el fin del mundo hace que la defensa de la regulación centralizada se contemple mucho mejor que en la mayoría de otros contextos, lo suficiente para haber convencido a algunos pensadores, entre los cuales Eric Drexler, de hacer al menos una excepción parcial con respecto a su usual preferencia hacia la descentralización, mercados privados, *laissez-faire*.

Mientras que la defensa de la centralización es, de algunas formas, más fuerte para una tecnología tan poderosa, también lo es la crítica. Solo ha habido una ocasión en mi vida en que haya pensado que hubiera una oportunidad significativa de que mis seres queridos y cercanos pudieran morir. Me ocurrió un poco después del ataque

---

[156] Tanto el diseño como el propósito son, por supuesto, metafóricos, puesto que la evolución no es un actor consciente. Pero la consecuencia de la evolución biológica (organismos diseñados como lo serían por un diseñador cuyo objetivo fuera el éxito reproductivo) es la misma que si fueran deliberados.

terrorista del 11 de septiembre, cuando comencé a investigar el tema de la viruela.

La viruela se había eliminado oficialmente; que se supiera públicamente, las últimas cepas del virus se encontraban en los laboratorios gubernamentales rusos y estadounidenses. Ya que había sido eliminada, y ya que la salud pública es un campo dominado por los Gobiernos, la vacuna contra la viruela también se había eliminado. Aparentemente no se le había ocurrido a nadie en posición de hacer nada al respecto que merecía la pena mantener la suficiente cantidad de copias de seguridad para revertir esa decisión rápidamente. EE.UU. tenía suministros de vacunas, pero eran adecuadas para vacunar a solo una pequeña parte de la población. Que yo sepa, tampoco nadie más tenía suministros sustanciales.

La viruela, en una población sin vacunar, produce tasas de mortalidad tan elevadas con un 30%. La mayoría de la población mundial se encuentra ahora sin vacunar; los vacunados hace cuarenta o cincuenta años podríamos o no estar todavía protegidos. Si un terrorista hubiera conseguido una copia del virus, robada de un laboratorio gubernamental o cultivada a partir de los cuerpos de víctimas de viruela enterradas en algún sitio del ártico en algún momento del pasado (nadie parece saber seguro si eso es posible), podría haberlo usada para matar a cientos de millones, quizás más de mil millones, de gente. Ese riesgo existía porque las tecnologías para protegernos contra los replicadores (esa clase particular de replicadores) habían estado bajo control centralizado. El centro había decidido que el problema estaba resuelto.

Por suerte, no sucedió.

DIECINUEVE

COMPAÑÍA PELIGROSA

Lo especial de la Humanidad se encuentra solo entre nuestras orejas; si vas buscándolo en cualquier otra parte, acabarás decepcionado.

Lee Silver[157]

Lo que soy y dónde se localiza en mi cuerpo es un rompecabezas muy viejo. Un intento temprano de responderlo mediante experimentación se describe en *Jomsviking saga*[158], escrita en el siglo XIII. Tras una batalla, se está ejecutando a los guerreros capturados. Uno de ellos sugiere que la ocasión proporciona la oportunidad perfecta para zanjar un argumento en curso sobre la localización de la conciencia. El condenado sostendrá un pequeño cuchillo hacia abajo mientras que los ejecutores cortan su cabeza con una afilada espada; tan pronto caiga su cabeza, intentará poner hacia arriba el cuchillo. Se necesitan unos pocos segundos para que muera un hombre, así que si su conciencia está en su cuerpo, lo conseguirá; si está en su cabeza, que ya no está unida a su cuerpo, fracasará. El experimento se desarrolla como se ha propuesto; el cuchillo cae boca abajo.

Todavía no sabemos con mucha seguridad qué es la conciencia, pero sabemos más sobre el tema que los jomsvikings. Parece claro que está íntimamente conectada con el cerebro. Un ordenador programado actúa más como una mente humana que cualquier otra cosa cuyo funcionamiento comprendamos. Y sabemos lo suficiente sobre el mecanismo del cerebro para interpretarlo plausiblemente como un ordenador orgánico. Ello sugiere una conjetura obvia e interesante: lo que soy es un programa o un conjunto de programas, *software*, ejecutándose en el *hardware* de mi cerebro. Las estimaciones actuales sugieren que el cerebro humano tiene una potencia de procesamiento mucho mayor que cualquier ordenador existente, así que no es

---

157 Silver, 1998.
158 Hollander, 1988.

sorprendente que los ordenadores solo puedan realizar un trabajo muy imperfecto imitando el pensamiento humano.

Esta conjetura plantea una posibilidad interesante y aterradora. Los ordenadores han estado doblando, durante los últimos treinta años o así, su potencia cada uno o dos años, un patrón conocido, en varias formulaciones distintas, como *la ley de Moore*. Si esa tasa de crecimiento continúa, en algún punto en el futuro no muy lejano (la estimación de Raymond Kurzweil es de unos treinta años), deberíamos ser capaces de construir ordenadores que sean tan inteligentes como nosotros.

Construir el ordenador es solo parte del problema; todavía tenemos que programarlo. Un ordenador sin *software*solo es un pisapapeles caro. Para obtener inteligencia al nivel humano en un ordenador, tenemos que encontrar alguna forma de producir el *software* equivalente a nosotros.

La forma más obvia es comprender cómo pensamos (de forma más general, cómo funciona el pensamiento) y escribir el programa en consecuencia. Los primeros trabajos de IA siguieron esa estrategia, intentando escribir*software* que pudiera realizar funciones muy simples del tipo que hacen nuestras mentes, como reconocer objetos. Resultó ser un problema sorprendentemente difícil, lo que dio a la IA una reputación de campo que prometía mucho más de lo que concedía.

Es tentador argumentar que el problema no solo es difícil, sino imposible, que una mente de un nivel dado de complejidad (cómo se definiría eso no está claro) solo puede comprender cosas más sencillas que ella misma, y, por tanto, no puede entender cómo funciona ella misma. Pero incluso si eso es cierto, no se sigue que no podamos construir máquinas al menos tan inteligentes como nosotros; uno no tiene que comprender cosas para construirlas. Nosotros mismos somos, para aquellos que aceptan la evolución en vez de la creación divina como la mejor explicación de nuestra existencia, un impresionante ejemplo de lo contrario. La evolución no tiene mente. Aun así, ha construido mentes, incluidas las nuestras.

Ello sugiere una estrategia para crear *software* más inteligente de un uso creciente en los últimos años. Crea una analogía virtual de la evolución, un sistema en que el *software* se encuentre sujeto a algún

tipo de variación aleatoria, que ha pasado pruebas según un criterio de éxito, y seleccionada según lo bien que cumple ese criterio. Repite el proceso un gran número de veces, usando el resultado de un estadio como aportación al siguiente. Mediante una versión de esa solución se creó al menos parte del *software* de reconocimiento facial, una habilidad informática discutida en un capítulo anterior. Quizás, si tuviéramos ordenadores lo bastante potentes, y alguna manera simple de juzgar la inteligencia de un programa, podríamos hacer evolucionar programas con inteligencia al nivel de los humanos.

Una segunda alternativa es revertir la ingeniería. Después de todo, tenemos muchos ejemplos de inteligencia a nivel humano disponibles. Si pudiéramos comprender con suficientes detalles cómo funciona el cerebro (incluso si no comprendiéramos del todo por qué funcionando de esa forma se obtuvo como resultado una entidad consciente e inteligente), podríamos imitarlo en silicio, construir una analogía en máquina de un cerebro humano genérico. Nuestros cerebros deben de autoprogramarse hasta un grado significativo, ya que la única información con la que comienzan se contiene en el ADN de una única célula fertilizada, así que con suficiente ensayo y error podríamos conseguir que nuestra imitación se despierte y aprenda a pensar. Quizás deberíamos poner a trabajar a un equipo en el problema del café digital.

Una tercera alternativa es revertir la ingeniería, no de un cerebro genérico, sino de uno particular. Supón que se pudieran construir sensores lo suficientemente buenos para construir un marco preciso de la estructura y el estado de un cerebro humano específico en un instante en particular: no solo qué neurona se conecta con qué otra y cómo, sino en qué estado se encuentra cada neurona. Entonces imitas precisamente esa estructura en ese estado en el*hardware*. Si todo lo que soy es *software* ejecutándose en el *hardware* de mi cerebro y puedes imitar completamente ese *software* y su estado actual en un *hardware* diferente, deberías tener una inteligencia artificial que, al menos hasta que evalúe datos que entren tras su creación, piense que soy yo. Esa idea, comúnmente descrita como «subir» un ser humano, plantea un gran número de preguntas,prácticas, legales, filosóficas y morales. Se vuelven especialmente interesantes si damos por hecho que

nuestros sensores pueden observan mi cerebro sin dañarlo, dejando, tras la subida, dos David Friedmans, uno ejecutándose en carbono y otro, en silicio.

UN MUNDO NUEVO

Toto, tengo la impresión de que ya no estamos en Kansas.
Dorothy, *El mago de Oz*

Un futuro con inteligencia artificial al nivel de la humana, se produzca de la forma que sea, plantea problemas para los acuerdos legales, políticos y sociales existentes. ¿Tiene derechos legales un ordenador? ¿Puede votar? ¿Es asesinato matarlo? ¿Estás obligado a cumplir las promesas que le haces? ¿Es una persona?[159]

Supón que acabamos alcanzando lo que parece la conclusión obvia: que una persona viene definida por algo más fundamental que el ADN humano, o cualquier ADN en general, y que algunos ordenadores cumplen los requisitos. Ahora tenemos nuevos problemas: esa gente es diferente de algunas maneras muy fundamentales de toda la gente que hemos conocido hasta ahora.

Un ser humano está unido intricada e inextricablemente a un cuerpo humano. Un programa informático puede ejecutarse en cualquier *hardware* adecuado. Los humanos pueden dormir, pero si los apagas del todo, mueren. Puedes guardar el estado actual de un programa informático a tu disco duro, apagar el ordenador, encenderlo mañana y volver a ejecutar el programa. Cuando lo desenchufaste, ¿fue asesinato? ¿Depende de si planeaste o no enchufarlo de nuevo?

Los humanos dicen que se reproducen, pero no es cierto. Mi mujer y yo hemos producido hijos conjuntamente (ella hizo la parte difícil), pero ninguno de ellos es una copia precisa de ninguno de nosotros. Incluso con un clon, solo el ADN sería idéntico; las experiencias, pensamientos, creencias, recuerdos, personalidad serían los suyos.

---

[159] Para una discusión temprana de algunos de estos asuntos, véase Freitas, 1985. Más recientemente, los tribunales han mantenido que un ordenador no puede ejercer la ley en Texas: http://www.rfreitas.com/Astro/LegalRightsOfRobots.htm.

Un programa informático, por otra parte, puede copiarse a múltiples máquinas; incluso puedes ejecutar múltiplesejemplos del mismo programa en una máquina. Cuando se copia un programa que resulta ser una persona, ¿qué copia posee la propiedad de esa persona? ¿Cuál es el responsable de las deudas? ¿A cuál se castiga por delitos cometidos antes de la copia?

Tenemos fuertes normas legales y morales contra poseer los cuerpos de otras personas, al menos mientras están vivos. Pero un programa de IA se ejecuta en *hardware* que alguien construyó, que podría usarse para ejecutar otros tipos de *software*. Cuando alguien produzca la primera IA a nivel humano en un *hardware* puntero que cuesta muchos millones de dólares, ¿obtiene el programa la propiedad del ordenador en el que se está ejecutando? ¿Tiene un derecho legal a sus requisitos de por vida, más obviamente de potencia? ¿O pueden los creadores, dando por hecho que todavía tienen control físico sobre el *hardware*, grabarlo en un disco, apagarlo y empezar a trabajar en la versión del Mark II?

Supón que hago un trato con una IA a nivel humano. Le proporcionaré un ordenador apropiado al que transferirá una copia de sí mismo. A cambio, accede a que el año que viene la copia pasará la mitad de su tiempo (doce horas al día) trabajando gratis para mí. ¿Está atada la copia por ese acuerdo? «Sí» significa esclavitud. «No» es una buena razón por la que nadie proporcionará *hardware* para la segunda copia. No, al menos, sin mantener el derecho a apagarlo.

DEJANDO CAER EL OTRO ZAPATO

He estado discutiendo rompecabezas asociados con el problema de adaptar nuestras instituciones a la inteligencia artificial al nivel humano. No es un problema que probablemente que dure mucho.

Antes cité una estimación de Kurzweil sobre unos treinta años para llegar a la IA a nivel humano. Supón que tiene razón. Supón además que la ley de Moore sigue vigente, que los ordenadores siguen duplicando su potencia cada uno o dos años. En cuarenta años, eso les hace algo así como cien veces más inteligentes que nosotros. Ahora

somos chimpancés (quizás roedores) y más nos vale que a nuestros nuevos señores les gusten las mascotas.

La solución de Kurzweil es que nosotros también nos volvamos ordenadores, al menos en parte. Es probable que los desarrollos tecnológicos que lleven a una IA avanzada se asocien con una comprensión mucho mayor de cómo funcionan nuestros propios cerebros. Ello debería hacer posible construir interfaces de cerebro a máquina mucho mejores, permitiéndonos mover una parte sustancial de nuestro pensamiento a silicio. Piensa en 89 352 por 40 327 y la respuesta es, obviamente, 3 603 298 104. Multiplicar números de cinco cifras no es una habilidad tan útil, pero si comprendemos lo bastante sobre el pensamiento para construir ordenadores que piensen tan bien como nosotros, sea por diseño, evolución o ingeniería inversa, deberíamos comprender lo bastante para descargar partes más útiles de nuestro procesamiento de información de serie a *hardware* externo. Ahora también podemos aprovecharnos de la ley de Moore.

La versión extrema de este marco hipotético se funde con la subida. Con el tiempo, cada vez más cantidad de tu pensamiento se realiza en silicio, cada vez menos en carbono. Al final tu cerebro, quizás también tu cuerpo, lleva a representar un papel menor en tu vida, con lo que los órganos se mantendrían por sentimiento.

A falta de convertirnos nosotros mismos en ordenadores en parte o por completo o acabar como (si somos optimistas) mascotas de supermentes informáticas[160], veo otras tres posibilidades. Una es que el crecimiento continuo de la potencia informática que hemos observado en décadas recientes se encuentre con algún límite natural y se ralentice o pare. El resultado podría ser un mundo en el que nunca obtengamos IA al nivel humano. Menos plausiblemente, el proceso podría ralentizarse justo a tiempo, dejándonos con iguales pero no señores, y un futuro muy interesante. El único argumento que puedo ver para esperar ese resultado es que eso sea lo inteligentes que somos; quizás haya límites fundamentales para nuestra capacidad de

160 Las novelas de la serie de la cultura de Ian Banks dan cuenta mediante la ciencia ficción de una sociedad con gente como nosotros que son, en efecto, mascotas de inteligencias artificiales vastamente superiores.

pensamiento con los que nuestra especie se encontró hace unos pocos cientos de miles de años. Pero no me parece muy probable.

Una segunda posibilidad es que quizás no somos *software* después de todo. La analogía es convincente, pero hasta que hayamos comprendido en detalle cómo funcionamos o tengamos éxito en producir ordenadores programados mucho más como nosotros que los de hasta ahora, se queda en una conjetura. Quizás mi conciencia realmente es un alma inmaterial, o al menos algo descrito de forma más precisa como un alma inmaterial que como un programa ejecutándose en un ordenador orgánico. No apostaría por ello, pero podría ser cierto.

Por último, existe la posibilidad de que la conciencia, autoconciencia o voluntad dependa de más que una mera potencia de procesamiento, que sea una característica adicional que deba ser diseñada en un programa, quizás con gran dificultad. Si es así, la principal línea de desarrollo en la inteligencia artificial podría producir máquinas con inteligencia, pero sin iniciativa, esclavos naturales respondiendo solo las preguntas que ponemos en ellas, haciendo las tareas que fijamos, sin voluntad u objetivos propios. Si otro, siguiendo una línea diferente, produce un programa que sea una persona real, más inteligente que nosotros, con sus propias metas, podemos tratar de usar a nuestros esclavos robóticos para que lidien con el problema por nosotros. De nuevo, no me parece probable; las ventajas de una máquina que puede plantear preguntas por sí misma, formular metas, tomar decisiones parecen demasiado grandes. Pero podría estar equivocado. O podría resultar que la autoconciencia, por alguna razón, es un problema mucho más difícil que la inteligencia.

VEINTE

TODO EN TU MENTE

El espacio real solo lo es en el siglo XX.
Alguien, en algún lugar, en algún tiempo en la primera década del siglo veintiuno.

Hace algunos años di una charla en Italia por teléfono, desde mi despacho de mi casa de San José. Desde ahí me sentía un poco como hablar al vacío. Un año o dos más tarde repetí el experimento con mejor tecnología. Esta vez estaba sentado en una sala de videoconferencias. Mi audiencia de Países Bajos podía verme y yo podía verlos. Aun así no es muy real, pero se acerca mucho más.

La vez siguiente podría acercarse todavía más. No solo me ahorro el vuelo, sino que la audiencia también. Estoy en casa; ellos, también. Cada uno de nosotros lleva cascos y gafas, se encuentra frente a una pequeña videocámara. Las lentes de las gafas son pantallas de video; lo que veo no es lo que se encuentra frente a mí, sino lo que dibujan. Lo que están dibujando es una habitación llena de gente. Cada uno está viendo la misma habitación desde la otra dirección, observándome en una tarima virtual mientras pronuncio mi charla.

La realidad virtual no solo ahorra en vuelos, sino que también tiene otras ventajas. Mi ordenador procesa la imagen de mi videocámara antes de mandarla a toda mi audiencia. Eso me proporciona una oportunidad de mejorarla un poco antes, reemplazar mi albornoz por traje y corbata, darme un afeitado que necesito con ganas, quitarme una década o así. Mi audiencia también parece sorprendentemente atractiva, arreglada y bien vestida. Y mientras que, desde mi punto de vista, están distribuidos equitativamente por la sala, cada uno de ellos me mira desde el mejor asiento de su casa.

Hace mucho se me reveló el secreto de las charlas en público: siempre habla en una habitación un poco demasiado pequeña para la audiencia. En la realidad virtual, la escala es automática; el número de gente que aparece es el número de asientos de la sala. Y para cada uno de ellos, la

sala se encuentra diseñada de forma personalizada, con láminas de oro si su gusto es lo bastante fastuoso. En la realidad virtual, el oro es tan barato como cualquier otra cosa. Si no me crees, echa un vistazo a uno de los fragmentos más llamativos de un buen videojuego: la Represión del Odio del *Diablo II,* digamos.

Los videojuegos son nuestra forma más familiar de realidad virtual. Mirando la pantalla, ves un mundo que solo existe en la memoria del ordenador, representado por un patrón de puntos de colores en la pantalla. En ese mundo, múltiples personas pueden interactuar, y lo hacen, cada uno desde su ordenador. En los videojuegos en primera persona, cada uno ve en la pantalla lo que estaría viendo si fuera el personaje con el que juega. En algunos, el mundo virtual se completa con realistas leyes físicas. *Myth*, que yo sepa, calculaba el vuelo de cada flecha; si un enano lanzaba una granada colina arriba, bajaba rodando. A medida que la tecnología mejora, podemos esperar que vaya más allá del entretenimiento. Quizás debería mantenerme alejado de las acciones de las aerolíneas por un tiempo.

Ya sabemos cómo hacer todo lo que he descrito. A medida que los ordenadores se vuelven más rápidos y las pantallas de ordenador (incluyendo las que se proyectan en gafas), más nítidas, seremos capaces de hacerlo mejor y más barato. En una década, probablemente menos, deberíamos ser capaces de crear realidad virtual visual y sonora de forma barata con la resolución del mundo real, con un video lo bastante bueno para hacer convincente la ilusión. El sonido ya lo es.

Por muy buenas que sean nuestras pantallas, este tipo de realidad virtual sufre una seria limitación: solo engaña a dos sentidos. Con un poco más de trabajo, podríamos añadir un tercero, pero el olfato no representa un gran papel en nuestras percepciones. El tacto, el gusto y los sentidos kinestéticos que nos dicen lo que está haciendo nuestro cuerpo son un problema mucho más difícil. Si mi pantalla de ordenador es lo bastante buena, el villano podría parecer completamente real, pero si trato de golpearlo, me llevaré una sorpresa desagradable.

Nuestra tecnología presente para crear una realidad virtual depende de la fuerza bruta, usando las percepciones, el conjunto de herramientas con las que sentimos el mundo alrededor de nosotros. ¿Quieres oír cosas? Haz vibrar aire en el oído. ¿Quieres ver cosas?

Fotones luminosos en la retina. Aplicar esa solución al resto de los sentidos es más difícil. E incluso si pudiéramos hacerlo, todavía nos quedaría el problema de coordinar lo que nuestro cuerpo está haciendo en el espacio real con lo que estamos viendo, oyendo y sintiendo que hace en el espacio virtual.

HOY Y MAÑANA: EL MUNDO DE LA RV PRIMITIVA

Si juegas a videojuegos, la realidad virtual (la versión de fuerza bruta) ya es parte de tu vida. A medida que se vuelve más barato, un resultado será mejores videojuegos.

La comunicación es otra aplicación obvia. Todavía no serás capaz de acercar la mano y tocar a alguien, salvo metafóricamente. Pero ver y escuchar es mucho mejor que solo escuchar. Una conferencia por teléfono se vuelve más como un encuentro cuando puedes ver quién está diciendo qué a quién y leer las palabras encarnadas en las expresiones faciales y movimientos corporales.

Esto plantea un problema interesante. Todos, automáticamente y por rutina, juzgamos a la gente de alrededor no solo por lo que dicen, sino por cómo lo dicen: tono de voz, expresión facial, gestos. La mayoría de la gente no sabe mentir: esa es una de las razones por las que la sinceridad es la mejor película. Hacer que la gente crea que eres sincero mientras realizas las acciones que mejor sirvan a tus propósitos sería una política todavía mejor (para ti, no para la gente con la que tratas), pero para la mayoría de nosotros no es una solución práctica.

Llamamos a las excepciones estafadores. Son gente que, mediante talento o entrenamiento, han dominado la habilidad para divorciar lo que realmente están pensando y haciendo del sistema de signos no verbales, el monólogo de dentro de nuestras cabezas, que todos nosotros transmitimos continuamente. Por suerte, muchos son realmente buenos en esto.

Mi ordenador puede hacerme parece más joven. También podría ser capaz de hacerme parecer más sincero. Una vez alguien haya realizado un trabajo adecuado de desciframiento del lenguaje mediante el cual comunicamos pensamientos y emociones mediante expresiones faciales

y posturas corporales (que yo sepa, alguien ya lo ha hecho, seguramente alguien que pertenece al negocio de entrenar vendedores), podemos crear falsificadores informatizados. No tengo talento para mentir. Mi ordenador, por otra parte...

El otro lado del problema de los estafadores virtuales es que en Internet nadie sabe que eres un perro. O una mujer. O un niño de doce años. O tullido. En la realidad virtual, una vez funcione correctamente el *software* de edición a tiempo real, puedes hacer cualquier cosa que puedas imaginar. Mujeres caseras pueden ocultar su rostro; niños precoces pueden ser juzgados por la edad mental reflejada en lo que dicen y hacen, no por la edad física reflejada en sus caras. Cuando mi hijo de catorce años se mete en *World of Warcraft*, envejece cinco o seis años. Es una buena práctica.

Cuando interactúas en Usenet o un grupo de correo electrónico, estás proyectando una identidad, dando a los otros miembros del grupo una imagen mental del tipo de persona que eres. Hace algunos años, alguien sugirió un juego para el Newsgroup rec.org.sca: que los participantes escribieran y publicaran descripciones físicas de otros participantes que nunca hubieran conocido. Yo gané casi veintitrés centímetros. En la realidad virtual, nunca tengo que volver a ser bajo.

A menos, por supuesto, que quiera serlo.

Mi contribución a Corpore Sano

En el mundo moderno, ya no tenemos que preocuparnos mucho de escapar de depredadores o perseguir presas. Ya no tenemos que rascar en el suelo con palos gruesos para cultivar comida. Para la mayoría de nosotros, «trabajo» significa poco ejercicio físico. Pero todavía hay juegos: baloncesto, fútbol, tenis. Una objeción contra los videojuegos es que eliminan uno de los pocos incentivos que la gente moderna tiene para hacer ejercicio.

Observa a alguien, quizás a ti mismo, jugando a un videojuego absorbente. Como con otros juegos, el ganar prima sobre otras preocupaciones. Hace mucho descubrí el indicador de un juego de ordenador de primera clase: que cuando por fin dejé el ordenador para

usar el baño, fue porque de verdad tenía que hacerlo. Y muchos jugadores de muchos juegos se han dado cuenta de lo cansados que están sus pulgares solo cuando ha terminado el juego.

Si lo que quieres es hacer ejercicio, la solución obvia es mandos más grandes. Combina un videojuego con una máquina de hacer ejercicio. Usar la máquina controla lo que sucede en el juego. Como en el atletismo del mundo real, solo te das cuenta de lo cansado que estás después de que hayas ganado o perdido. Ya existen[161] implementaciones primitivas, sobre todo el *Dance Dance Revolution*.

En mi versión mejorada, los videojuegos se convierten en mejor ejercicio que los juegos reales porque el ambiente que crea el ordenador está hecho a medida, segundo a segundo, de las necesidades de tu cuerpo. La ambientación es el Pacífico durante la Segunda Guerra Mundial. Estás controlando un arma antiaérea en el *Yamato*, el navío de guerra más grande del mundo, tratando desesperadamente de defenderlo contra las oleadas de bombarderos estadounidenses que intentan destruir mediante pura fuerza bruta la gloria de la marina japonesa. Mueves el arma de izquierda a derecha con los brazos, bajas o elevas el cañón con los controles del pie; cuando sueltas los controles, vuelve al centro. Tu fuerza está moviendo físicamente el arma, así que no es sorprendente que sea mucho trabajo.

Tras la tercera oleada, el ordenador que controla el juego se da cuenta de que estás teniendo problemas para mover el arma rápidamente a la izquierda: tu brazo izquierdo se está cansando. El siguiente ataque viene de la derecha. A medida que el brazo derecho se va cansando igual, cada vez más ataques exigen que ajustes la elevación del arma, cambiando el trabajo a las piernas. Cuando el ritmo cardiaco alcance el límite superior de la zona aeróbica, hay un parón en el ataque, durante el cual escuchas música militar. Cuando se aminore el ritmo cardiaco,

---

[161] http://www.cbsnews.com/stories/2002/06/13/earlyshow/contributors/tracysmith/main512169.shtml, http://www.halfbakery.com/idea/Arcade20Treadmill. Quizás sea más interesante Nintento Wii, un videojuego cuyo controlador está diseñado para que tu personaje en la pantalla copie tus acciones en el mundo real (al menos hasta el punto de seguir el movimiento de tu mano). EyeToy de Sony consiguió un efecto similar usando una cámara para observar tus movimientos y decirle a la PlayStation 2 a la que estaba enlazada qué estabas haciendo.

llega la siguiente ola. El tenis puede ser diversión y ejercicio, pero el arte, el que está bien hecho, es mejor.

Un juego de ejercicio sofisticado es una forma con la que podemos utilizar la realidad virtual. Otra es hacer cosas peligrosas mientras que solo se nos mata virtualmente. Piensa en el problema de la ingeniería en ambientes peligrosos: el fondo de la fosa de las Marianas, digamos, a ocho kilómetros bajo las olas, o en la superficie de la luna. Una solución es que el que opera el equipo esté ahí solo virtualmente. Su cuerpo se encuentra en un ambiente seguro, llevando gafas, manipulando controles. Su punto de vista, como en un videojuego en primera persona, es el punto de vista de la máquina que está operando.

En el caso de la Luna, tenemos un pequeño problema técnico: la velocidad de la luz. Si el operador está en la Tierra y la máquina, en la Luna, habrá un retraso perceptible cuando la máquina le mande información y cuando su respuesta, basada en esa información, vuelva a la máquina. A algunos de nosotros nos han matado virtualmente por dichos retrasos en videojuegos. En el caso de la ingeniería lunar, mientras que la muerte sería solo virtual para el operador, podría ser real para la máquina, y colocar *hardware* en la luna no es barato. Quizás deberíamos poner también al operador en la luna, o en órbita alrededor de ella, en algún lugar más seguro que el túnel que está cavando, más cercano que la Tierra.

Como sugieren estos ejemplos, la realidad virtual, incluso implementada usando las tecnologías rudimentarias que tenemos ahora, puede tener usos importantes en el mundo real.

RV PROFUNDA: MÁS ALLÁ DEL PROBLEMA DE SOÑAR

Una solución elegante a los límites de esas tecnologías es la forma de realidad virtual que la mayoría de nosotros experimentamos cada noche. En un sueño, cuando dices a tu brazo que se mueva, tu brazo virtual se mueve. El real (normalmente) no lo hace. Los sueños no se limitan a visión y sonido. Supón que conseguimos descifrar el problema del sueño, que descubrimos lo suficiente sobre cómo funciona el cerebro para que también nosotros podamos crear ilusiones con todos

los sentidos. Tenemos RV profunda. Cualquiera que la quiera tiene un enchufe en la parte posteriordel cuello. Las señales a través del cable enchufado a ese enchufe pueden crear una ilusión con todos los sentidos de cualquier cosa que nuestros sentidos podrían haber experimentado.[162]

Pensando en el mundo que esa tecnología hace posible, un primer paso útil es distinguir entre transacciones de información y transacciones materiales. Leer este libro es una transacción de información. El libro es un objeto físico. Pero leer la ilusión de un libro, con las mismas palabras en las páginas virtuales, podría valer igual. Cuando sostienes una conversación, estás usando cuerdas vocales físicas para hacer vibrar el aire físico de forma que transmita lo que comunicas y estás usando un tímpano físico para recoger esas vibraciones de forma que recibas lo que comunica la otra persona. Pero ese aparato es meramente la maquinaria para transmitir información. Las señales electrónicas que crearon la ilusión de que tu voz decía esas mismas palabras conseguirían el mismo efecto.

Para una transacción material, piensa en cultivar trigo. Podrías cultivar trigo virtual, tener la experiencia sensorial de plantar, arrancar las malas hierbas, cosechar. Pero si intentaras vivir del trigo virtual que cultivaste, podrías acabar muriendo de hambre real. La gente del *World of Warcraft* cocina comida virtual y fabrica armas y armaduras virtuales. Pero no sirve de mucho fuera del juego.

Una forma de realidad virtual suficientemente avanzada puede proveer para todas las transacciones de información. Podría ayudar con algunas transacciones materiales: la cosechadora podría dirigirla un operador que se encontrara en otra parte, dando instrucciones reales a una máquina real. La presencia física del operador sería una ilusión, la información que está usando, real, proporcionada por cámaras y

---

[162] En http://www.cbsnews.com/stories/2003/10/13/tech/main577757.shtml se describe un experimento en el que se entrenó a monos con implantes cerebrales para mover un brazo robótico con sus pensamientos. Una propuesta más simple que ahora se ha estado usando para varios pacientes con brazos protéticos transfiere mediante cirugía las terminaciones nerviosas del hombro al pecho, de forma que las señales nerviosas que normalmente controlarían el brazo que falta en lugar de ello provoquen una contracción en el pecho, que manda una señal al brazo protético. http://www.washingtonpost.com/wp-dyn/content/article/2006/09/13/AR2006091302271 pf.html, http://www.danishtechnology.dk/robot/20163,3.

micrófonos en la cosechadora. Pero si quieres que las transacciones reales produzcan resultados, comida, casas o cualquier otra cosa real, alguien o algo tiene que hacerlas de verdad.

Teletranspórtame, Scotty

En *Star Trek*, la gente se teletransporta de un sitio a otro. No conozco ninguna razón para esperar que suceda, y si así fuera, sería reacio a hacerlo, ya que no está claro si usarlo es transporte o suicidio: yo muero y la máquina crea una copia que piensa que soy yo. Pero mientras que todo cuanto movamos sea información, la realidad virtual puede servir evitando los problemas filosóficos.

¿Por qué quiero visitar a mis amigos? Para verlos, sentirnos, para escucharlos, hacer cosas con ellos. A menos que una de las cosas sea construir una casa o plantar un jardín que realmente deba construirse o plantarse, toda la visita es una transacción de información. Con una buena RV, mi cuerpo se queda en casa y mi mente es la que recorre el camino. Si te parece una idea rara, piensa en una llamada de teléfono: también es un sustituto de la visita. La RV simplemente incrementa al ancho de banda para cubrir todos nuestros sentidos, proporcionando una forma de que un grupo de dos o más personas se reúnan para cualquier transacción de información en la que deseen tomar parte —un encuentro, una conferencia de paz, un juicio, una aventura amorosa—.

Y ya que todo lo que sucede es información yendo y viniendo por redes sociales, información que puede encriptarse en el momento, volvemos a un mundo de privacidad férrea. La tecnología de vigilancia puede hacer público todo lo que suceda en el espacio real, pero ya no necesitamos hacer mucho ahí.

Ficción futura

El potencial para la industria del entretenimiento es igualmente impactante. Las obras de ficción se pueden experimentar con toda la

vista, oído y tacto, sin necesidad de imaginación. Si eso es una mejora es algo que no está claro; mi hija hasta ahora se ha negado a ver la versión cinematográfica de *La comunidad del anillo* porque prefiere el producto de su imaginación al producto de la imaginación del director. Los juegos de rol se volverán mucho más vívidos cuando llegues no solo a ver y escuchar a los monstruos, sino también a sentirlos, olerlos y tocarlos. Lo vívidas que sientas las garras del monstruo rajándote en tiras será una de las opciones del menú de opciones; yo elegiría un nivel de sensación bajo en este caso.

Una forma de entretenimiento virtual será un trabajo de ficción. Otra podría ser una grabación. Puedes escalar el Everest, hundirte en las profundidades del mar. Si hay guerras de verdad, unos pocos soldados podrían estar pluriempleados en el cine, grabando todo lo que les pasa. La pornografía por fin se convertirá en una seria competición para el sexo.

En cualquiera de estos casos, estamos creando como ilusión el tipo de experiencias que ya existen en la realidad. Piensa en cambio en una sinfonía. No se corresponde con nada de la naturaleza. El compositor ha cogido un sentido, el oído, y lo ha usado para crear una experiencia estética de su propia cabeza. Será interesante ver lo que un artista puede hacer con todos los sentidos.

Cuando estás experimentando la ficción de la RV, una pregunta es lo real que quieres que parezca. Mientras sucede la historia, ¿sabes que es una historia? ¿Hay una lucecita roja en el margen de tu visión periférica para decirte que nada de eso es real? Quizás la experiencia sería más conmovedora, más profunda, mejor arte, si pensaras que es real. Como un sueño.

Fantasía: sustituto o complemento

La realidad virtual, incluso en su forma actual, te permite hacer muchas cosas que la mayoría de nosotros preferiría que la gente no hiciera en el mundo real. Por ejemplo, los personajes del *World of Warcraft* pasan mucho tiempo pegando palizas a gente y cogiendo sus cosas. Si el juego hubiera existido hace veinte años, esperaría que la

gente a la que se pegara hubiera sido toda ella hombres, al ser más socialmente aceptada la violencia entre hombres que entre un hombre y una mujer. Sin embargo, bajo las normas actuales, la discriminación por género no se da; un jugador masculino se puede encontrar pasando gran parte de su tiempo dando palizas a mujeres (virtuales).

Ello plantea una pregunta obvia: habiendo golpeado por rutina a mujeres virtuales en línea, ¿estará ese jugador más dispuesto a golpearlas en el mundo real? Esa es una vieja pregunta, porque la realidad virtual es una tecnología vieja, aunque ahora la hayamos mejorado mucho. George Orwell, escribiendo hace más de sesenta años, se preocupó por el efecto corruptor sobre los lectores de la brutalidad común de la ficción criminal estadounidense;[163] los libros también son una forma de realidad virtual, aunque dejan gran parte del trabajo a la imaginación del lector. Más tarde, los escritores se preocuparon del efecto de la televisión. La última preocupación es el efecto del porno en Internet.

Desde el punto de vista de un economista, la cuestión es simple y empírica: ¿es el sexo y la violencia virtual un complemento o un sustituto del sexo y la violencia real? Si ves una película violenta, ¿hace eso que estés más dispuesto a que tú mismo cometas actos violentos, o identificarte con James Bond en la pantalla satisface tus deseos de violencia y excitación sin las consecuencias inconvenientes de actuar así por tu cuenta? ¿Hace la pornografía en línea que describe violaciones, esclavitud, tortura sexual y otras cosas reprobables que sea más probable que el lector realice dichos actos o menos?

Durante mucho tiempo, las pruebas sobre el tema (en parte motivadas por la búsqueda de argumentos a favor de censurar la pornografía que mostrara violencia contra las mujeres) consistían en experimentos altamente artificiales en los que se mostraban películas pornográficas y luego se preguntaba si se habían visto afectadas sus actitudes frente a la violencia sexual. Ahora, sin embargo, tenemos algunos datos del mundo real, gracias a un trabajo ingenioso de Tod Kendall.[164] Se le

---

[163] "Raffles and Mrs. Blandish," en Orwell, 1968, pp. 212–224, en http://www.george-orwell.org/Raffles and Miss Blandish/0.html.

[164] Tod Kendall, «Pornography, Rape, and the Internet,» actualmente en http://www.law.stanford.edu/display/images/dynamic/eventsmedia/Kendall%20cover%20+%2

ocurrió que Internet había incrementado con mucho la disponibilidad de pornografía y, así, proporcionaba un experimento natural sobre sus efectos: correlaciona el crecimiento del acceso a Internet con los cambios en la frecuencia de las violaciones. Resultó que la correlación era negativa; los incrementos en la disponibilidad de Internet, y, por tanto, del porno en Internet, se asociaban con descensos en las tasas de violación. No existía un patrón similar con el asesinato. Ello proporciona alguna prueba de que el sexo violento virtual es un sustituto del sexo violento real.

No sabemos, por supuesto, si lo mismo será cierto para el sexo y violencia virtuales altamente mejorados que serían posibles con una profunda RV, pero el estudio proporciona al menos motivos limitados para el optimismo.

Lo que importa

He estado haciendo un boceto de lo que podría hacer la RV profunda. Si no te estás preocupando todavía, piensa en la versión a gran escala.

Se deben producir cosas reales, pero los seres humanos no necesitan muchas cosas para seguir vivos. Para comer, elige la harina a granel, aceite y lentejas más baratos que puedas encontrar. Calcula cuánto costarían al día dos mil calorías de cada uno. Ahora tienes una estimación aproximada de la dieta a más bajo coste alta en carbohidratos, grasas o proteínas, lo que prefieras. Para estar seguro, mete un gran bote de vitaminas. Podría no saber muy bien, pero el sabor ya no importa. Comer es una transacción material, el sabor es una transacción informativa. Graba en realidad virtual diez mil comidas de los mejores restaurantes del mundo y tus lentejas son de repente filete miñón, sushi, helados sundaes. Más de lo mismo sucede con otras exigencias materiales. Mi cuerpo ocupa solo medio metro cuadrado, o uno, de espacio. Con una mente libre para recorrer el universo virtual, ¿quién necesita un salón, o incluso una cama doble?

0paper.pdf. El autor proporciona sustancialmente más pruebas para esta conclusión que mi breve resumen.

Visto desde el espacio real, no es un mundo magnífico. Todos comiendo la comida más barata que mantendrá el cuerpo humano en buenas condiciones, viviendo en el equivalente humano de un espacio de almacenamiento de un aeropuerto que funciona con monedas, haciendo ejercicio solo moviéndote contra máquinas de resistencia, quizás como parte de juegos de realidad virtual, quizás bajo control automático mientras la mente está en otra parte.

Para la gente que vive en él, es el paraíso. Todas las mujeres son bellas, y las suficientes son serviciales. Todos los hombres son atractivos. Todos viven en una mansión que se puede redecorar al gusto, con láminas de oro si se desea.[165] Cualquiera, en cualquier lugar, cualquier experiencia que se tenga en mente, cualquier vida que se pueda crear en forma de ilusión, está a solo un instante. Come todo lo que quieras y no engordes un kilo.

¿Suburbio o paraíso? Depende de lo que importe. Si todo lo que importa es la sensación, lo que percibes, es un paraíso, incluso si no es obvio en una inspección superficial.

Como prueba en contra, piensa en una forma muy vieja de sexo virtual: la masturbación. En tu mente puedes estar haciendo el amor a la mujer de tus sueños, al menos si tienes una imaginación lo bastante buena. El orgasmo, las sensaciones físicas dentro de tu cuerpo, las señales nerviosas que llegan a tu cerebro, son reales. Aun así, incluso con la tecnología mejorada de los libros y videos pornográficos, hay algo que falta.

Si lo que importa es lo que experimentamos, el mundo que he descrito es un paraíso. Si lo que importa es lo que pasa de verdad, la situación es más complicada. Haciendo que alguien lea un libro que he escrito, que lo disfrute y le persuadan mis ideas me agrada lo mismo que si lo lee en la realidad virtual (como hacen los que están leyendo este libro en la Web). Pero ¿y el mero hecho de pensar que alguien leyó mi libro? ¿Y si me despierto de una larga vida como autor de éxito, estrella del baloncesto, cantante de ópera o Casanova para descubrir que todo fue un sueño? ¿Es tan bueno como lo real? ¿Está bien siempre que me muera antes de despertarme?

---

165 Algunos lectores podrían recordar el mundo descrito en Lewis, 1946. Por alguna razón, lo llamó «Hell» (infierno).

Robert Nozick, en *Anarquía, Estado y utopía*, planteó la pregunta en términos de una máquina de experiencias imaginaria, su versión de la RV.[166] Enchufa a alguien y tendrá experiencias tan vívidas y tan convincentes como en la vida real. Toda una vida de ellas. Supón que el propietario de la máquina de experiencia de alguna forma sabe la vida que vas a vivir y puede ofrecerte una versión ligeramente mejorada. Enchúfate en su máquina para una vida imaginaria en la que los bebés lloren un poco menos, tu salario sea un poco más elevado, tu carrera en una firma con un poco más de estatus. Si le crees, ¿aceptas el trato? ¿Cambias una vida real por una ficticia? ¿Lo que importa es criar niños, tener una carrera, plantar árboles frutales, escribir libros… o lo que importan son los sentimientos que tienes por hacer todas esas cosas?

Tendrás que decidir por ti mismo. Yo no lo tocaría ni con un palo.

EPÍLOGO: Y AHORA TENEMOS UN GANADOR

Un boceto temprano de este libro, incluyendo este capítulo, se escribió y se subió a la web en 2002. Por aquella época no tenía ni idea de cuál de los futuros que estaba discutiendo llegaría antes; si hubiera tenido que adivinar, probablemente habría apostado por el de la privacidad férrea posibilitada por la encriptación en clave pública.

Ahora lo sabemos. El mundo de la realidad virtual está aquí, posibilitado no por la tecnología primitiva actual de los sensores de movimiento y gafas de video, ni por la tecnología futura de interfaces mente/máquina, sino por la tecnología vieja y avanzada de la imaginación humana. Resulta que una pantalla plana y un altavoz son suficientes, siempre que el ambiente al que permitan acceder sea lo bastante interesante y atractivo.

A principios de 2007, *World of Warcraft* tuvo más de diez millones de suscriptores, incluyendo a los cinco miembros de mi familia inmediata. Contando con todos los juegos multijugador, se estima que el número total de jugadores en todo el mundo es al menos de cien millones. Los «granjeros chinos», gente en países pobres que intenta ganarse la vida

---

[166] Nozick, 1974, pp. 42–45.

jugando a esos juegos, ganando dinero virtual y bienes virtuales y cambiándolos en línea por dinero real, se estima en cientos de miles.[167]

El *World of Warcraft* es una fantasía, un trabajo de ficción, una historia construida en la que el jugador se sumerge en un personaje que interactúa con otros, tanto personajes manejados por otros jugadores como por el ordenador.*Second Life* es una variante diferente, y, de alguna forma, más interesante, de esta idea. Lo que ofrece no es una historia, sino un mundo, un marco, en el que los participantes pueden diseñarse a sí mismos y construir cosas, comerciar con los otros, interactuar de una amplia variedad de formas. Desde un punto de vista, es una versión de fuente abierta del tipo de juego más tradicional, construido por los participantes. Desde otro, es un primer paso hacia un sustituto plausible, para la mayoría de la gente la mayor parte del tiempo, del mundo real.[168] Y puesto que la RV tiene sitio para un número ilimitado de mundos, es un sustituto que podría hacer real la idea de utopía de Robert Nozick[169]: una amplia variedad de comunidades distintas dirigidas por distintos gobiernos, en las que cada individuo es libre para elegir la que prefiera.

Mientras que los juegos multijugador en línea son el ejemplo más impactante de la realidad virtual actual, hay otro que es un poco más viejo y mucho más sorprendente. Cuando veías a alguien caminando por la calle hablando a una persona invisible, sospechabas que estaba loco. Ahora, das por hecho que está utilizando su teléfono móvil. Cuando estás sosteniendo una conversación con alguien que se encuentra objetivamente a muchos kilómetros, pero subjetivamente justo a tu lado, estás participando en una versión (con un ancho de banda muy bajo) de la realidad virtual.

---

[167] Castronovo, 2006, proporciona una discusión interesante, aunque ya ligeramente pasada de moda, sobre los juegos en línea multijugador. Para una descripción de la granja de oro en junio de 2007, véase http://www.nytimes.com/2007/06/17/magazine/17lootfarmers-t.html?ex=1339732800&en=1676d344608cb590&ei=5090&partner=rssuserland&emc=rss. Para comentarios interesantes realizados por Steven Levitt, véase http://freakonomics.blogs.nytimes.com/2007/06/19/goldfarmers-on-the-web/.

[168] Una versión no ficticia de un mundo así, el Metaverso, se presenta en la novela de ciencia-ficción ingeniosa, entretenida y no muy seria de 1992 de Neil Stephenson, *Snow Crash*. Una versión anterior aparece en la novela rosa de 1987 de Vernor Vinge *True Names*, mencionada en el capítulo 3 como, quizás, la descripción más temprana de la importancia del anonimato en línea.

[169] Nozick, 1974, capítulo 10.

«El ciberespacio está donde tiene lugar una llamada de teléfono.»

VEINTIUNO

LA FRONTERA FINAL

De algunas formas, el futuro ha sido una gran decepción. Cuando leí por primera vez ciencia ficción, los viajes espaciales eran casi una característica definitoria del género, interplanetarios al menos; con suerte, interestelares. Otras tecnologías están más avanzadas respecto a lo previsto: los ordenadores son mucho más pequeños de lo que la mayoría de los autores esperaban y se usan para una variedad mucho más amplia de propósitos cotidianos, y la ingeniería genética de los cultivos ya es una realidad. Pero el uso serio del espacio se ha limitado a la órbita cercana a la Tierra: nuestro patio. Ni siquiera la actividad científica ha llevado a los humanos a una breve visita a la Luna. Hemos mandado unas pocas máquinas pequeñas un poco más lejos, y hasta ahora eso es todo.

Una posible explicación es que la lenta tasa de crecimiento se debe al papel dominante de los gobiernos, en sí un resultado de las obvias aplicaciones militares, en parte. Otra es que ir al espacio era mucho más difícil de lo que pensaban los autores. El problema con la última explicación es que ya hemos hecho la parte difícil. Los siguientes pasos, ahora que hemos aprendido a liberarnos del terrible estorbo de la gravedad terrestre, deberían ser mucho más fácil. Quizás, tras una breve pausa para descanso y refrigerio, estemos ahí.

VISTAS DESDE EL FONDO DE UN POZO

En una de las historias de ciencia ficción más improbables de Poul Anderson,[170] un hombre y un cuervo se transportan con éxito de un asteroide a otro en una nave impulsada por varias latas de cerveza. Por lo que sé del autor, probablemente realizó los cálculos para asegurarse de que la cosa funcionaría.

---

[170] Nozick, 1974, capítulo 10.

No habría llegado muy lejos en la Tierra, pero moverse en el espacio es, de algunas formas, un problema mucho más sencillo. Nuestro hogar en el presente se encuentra situado incómodamente en el fondo de un pozo muy profundo. Salir de ese pozo, elevar algo desde la superficie de la Tierra al espacio, requiere mucho trabajo. El precio, el coste de lanzamientos de satélites y servicios similares, se mide en miles de dólares por cada kilo y medio. Los escritores de ciencia ficción de los cincuenta y sesenta daban por hecho que el objetivo de salir de la Tierra era llegar a Marte, o Venus, o quizás a un planeta que orbita alrededor de una estrella distante. En algún momento entre entonces y ahora se le ocurrió a alguien que tenía poco sentido trepar, con un esfuerzo enorme, fuera de un pozo solo para tirarse a otro. Los planetas son trampas.

Una alternativa es un hábitat orbital, una nave espacial gigantesca localizada permanentemente en órbita alrededor de un planeta o estrella. La ecología de un mundo en miniatura de esa índole, como la ecología del hábitat orbitante en que ahora vivimos, consistiría en órbitas cerradas que obtienen su energía del Sol, reutilizando la energía en un equilibrio casi total.

El primer problema es dónde colocarlo. Una órbita solar, a menos que se encuentre muy cerca de la de la Tierra, en cuyo caso será inestable debido a la gravedad de la Tierra, está muy lejos. Orbitar alrededor de la Tierra, lo bastante lejos para evitar el caos de satélites de comunicaciones y basura orbital, parece más atractivo. Por desgracia, una órbita así se acabará viniendo abajo, aunque no tan rápido en el mundo real como en Star Trek.

Las soluciones son los puntos lagrangianos 4 y 5, L4 y L5 para abreviar. Son localizaciones en órbita alrededor de la Tierra sesenta grados delante y detrás de la Luna. Como Joseph Louis Lagrange demostró en 1772, son puntos de equilibrio estables. Un satélite o un hábitat espacial situado en L4 o L5 se queda ahí. Como una bola en el fondo de una fuente, si algo la empuja y mueve un poco del centro, vuelve a su posición inicial.

Un segundo problema es de qué construir el hábitat espacial: a cinco mil dólares el kilo y medio, los materiales de la Tierra son un poco caros. Ello sugiere una localización alternativa: el círculo de asteroides,

que consiste en un gran número de trozos de roca localizados entre las órbitas de Marte y Júpiter. Si no queremos vivir tan lejos de casa, podríamos usar asteroides fuera del cinturón, algunos de los cuales tienen órbitas que se acercan mucho a las de la Tierra.

Los asteroides son lo suficientemente pequeños, así que su gravedad es insignificante. Muchos son lo bastante grandes para proporcionar cantidades adecuadas de material para construir. Una forma de usar ese material sería colonizar un asteroide, quizás cavar túneles en su interior. Una alternativa, para aquellos que prefieran un viaje más corto al vecindario del planeta de origen, es convertir en mina un asteroide y mandar lo que se obtenga a algún lugar cercano a la Tierra, digamos, L5. Hay un largo camino desde el cinturón de asteroides hasta la Tierra, pero el transporte es más fácil si no comienzas en el fondo de un pozo. Enviar material desde el cinturón de asteroides podría llevar meses, incluso años, pero las fuerzas necesarias son mucho menores que las que se necesitan para levantar la misma cantidad desde la Tierra. Si no tienes mucha prisa, incluso podrías probar con cerveza.

Un futuro en el que un número significativo de personas son residentes permanentes del espacio, que viven en hábitats, asteroides, quizás en flotas de naves extractoras, plantea algunos asuntos interesantes. La cuestión política obvia es quién los dirige. ¿Son los equivalentes a los barcos en el alto mar, Estados independientes, u otra cosa? Un asunto legal y económico menos obvio es cómo definir y ejecutar los derechos de propiedad relevantes para una órbita (ya es un problema para los satélites de comunicaciones), trozos de materia flotando por el espacio, luz solar como energía, o demás cosas que sean escasas y útiles.

Hasta ahora la única razón que he ofrecido para vivir en el espacio es que es mucho más sencillo llegar al espacio desde allí. Se podría recordar a los lectores el hombre que explicó a sus amigos que jugaba al golf para seguir en forma; cuando le preguntaron por qué se mantenía en forma, respondió «golf». Hay respuestas mejores. Un ambiente con gravedad cero y un suministro ilimitado de vacío casi perfecto podría ser útil para algunas formas de producción. Los asteroides podrían proporcionar una fuente muy grande y barata de materias primas. Si bien su primer uso será construir cosas en el espacio, no tenemos que

detenernos ahí. Bajar cosas a un pozo es mucho menos trabajoso que subirlas.

Otra respuesta es que, si se satura la Tierra, podría ser necesario contemplar otros lugares donde vivir. Explotando una cadena de asteroides podríamos construir estructuras que proporcionarían espacio para vivir para muchísima más gente de la que hay ahora. No habrá carencia de energía; la luz del Sol que cae a la Tierra es menos de una milmillonésima parte del total emitido por el Sol. Una civilización lo bastante desarrollada que viaja por el espacio podría usar el resto. En el caso límite, uno podría imaginarse el Sol completamente rodeado por las obras del hombre, visible desde otras estrellas solo por la vasta emisión infrarroja del calor de nuestros desperdicios. Freeman Dyson ha propuesto localizar especies tecnológicamente sofisticadas un poco por delante de nosotros buscando en los cielos estrellas así.

La respuesta final es que hay riesgos al poner todos nuestros huevos en una cesta. Es posible, si bien no probable, que la vida en la Tierra mejore durante las próximas décadas. Pero es de todo menos cierto. Uno puede imaginarse una gama de posibles catástrofes, desde la plaga gris hasta el Gobierno mundial, que haría de cualquier otro sitio una opción muy atractiva. Hay mucho espacio en el espacio.

La barrera más grande para el futuro que he estado bosquejando es el coste de salir de la Tierra. Aunque una civilización espacial, una vez iniciada, podría autosustentarse, requiere un gran comienzo. Y a cinco mil dólares el kilo y medio, no es probable que muchos de nosotros vayamos.

Lo que plantea la pregunta obvia de si podría haber formas mejores que a bordo de un cohete gigante.

COGE UNA CUERDA MUY LARGA…

Artsutanov propuso usar el cable inicial para que se multiplicara a sí mismo, en un tipo de operación que empieza con pocos recursos o ninguno, hasta que llegara a plegarse mil veces. Luego, calculó, sería posible asir quinientas toneladas por hora o doce mil toneladas al día. Cuando piensas en que esto es casi equivalente a un vuelo Shuttle cada

minuto, apreciarás que el Camarada Artsutanov no está pensando en la misma escala que la NASA. Pero si uno extrapola de Lindbergh al estado del tráfico aéreo transatlántico de cincuenta años después, ¿nos atrevemos a decir que es demasiado optimista? Sin duda es una pura coincidencia, pero el sistema que Artsutanov prevé podría aguantar el incremento diario actual de la población mundial, permitiendo los veintidós kilogramos de equipaje permitidos por emigrante…

Arthur C. Clarke[171]

Para una forma realmente eficiente de transporte, piensa en un humilde ascensor. Elevar el ascensor mismo no requiere casi energía, ya que a medida que sube la caja, el contrapeso baja. El consumo de energía se reduce a casi su mínimo absoluto: la energía necesaria para elevar a los pasajeros de un punto a otro más alto. Y si el diseño es lo bastante bueno, puedes recuperar la mayor parte de esa energía cuando vuelven a bajar.

La idea de aplicar esta solución al transporte espacial, como el método menos eficiente que usamos actualmente, se debe a un ruso. Tsiolkovsky propuso por primera vez un cohete con múltiples niveles en 1895. El ascensor espacial lo planteó por primera vez Yuri Artsutanov, un ingeniero de Leningrado, en 1960, y se ha inventado de forma independiente al menos media docena de veces desde entonces.

Comienzas con un satélite en órbita geosincrona, sobre el ecuador, moviéndose en la dirección de la rotación de la Tierra, dando la vuelta una vez al día. Desde el punto de vista de alguien que se encuentra en el suelo, está quieto, ya que orbita la Tierra con la misma velocidad que rota el planeta.

Se dejan salir dos cables de este satélite, uno que sube y otro que baja. Para el que sube, la fuerza centrífuga sobrepasa la gravedad, así que intenta hacer subir el satélite. Para el que baja, la gravedad puede con la fuerza centrífuga, así que empuja hacia el otro lado. Se sueltan los cables a la velocidad adecuada y los dos efectos se equilibran exactamente. Se sigue sacándolos hasta que el más bajo toque el suelo. Se fija en una isla apropiada. Se pone un ascensor en él. Ahora tienes

---

171 Esta cita, y otras del capítulo, están sacadas de Clarke, 1981, en http://www.spaceref.com/news/viewnews.html?id=844.

una forma de llegar al espacio por unos dólares el kilo en vez de miles de dólares el kilo.

El ascensor espacial tiene una serie de características curiosas e interesantes, a algunas de las cuales llegaremos en breves. Por desgracia, construirlo se enfrenta a un problema técnico muy serio: encontrar algo lo bastante fuerte y lo suficientemente ligero para hacer una cuerda muy grande.

Piensa en un cable de hierro colgando verticalmente. Si es más largo de cincuenta kilómetros, su peso excede su fuerza y se rompe. Hacer el cable más gordo no ayuda, ya que cada vez que duplicas su fuerza también duplicas su peso. El kevlar, usado para fines que incluyen vestimentas a prueba de balas, es considerablemente más fuerte respecto a su peso que el hierro. Un cable de kevlar puede llegar a unos doscientos metros hasta que se rompa por su propio peso. La órbita geosincrona se encuentra a treinta y cinco mil kilómetros de alto. El kevlar no va a conseguir llegar.

A primera vista, parece que necesitamos un material casi doscientas veces más fuerte respecto a su peso que el kevlar, pero la situación no es tan mala. A medida que vas subiendo por el cable, te vas alejando de la Tierra, la gravedad se va debilitando y, ya que el cable da vueltas con el satélite (y la Tierra), la fuerza centrífuga se va haciendo más fuerte. Para cuando se llega al satélite, las dos se encuentran en equilibrio. Así que solo la parte inferior del cable será realmente pesada. Por tanto, cuando más se baje en el cable, menor peso hay debajo para aguantar, así que se puede hacer un cable más largo antes de que se rompa estrechándolo. Construir un ascensor espacial requiere algo mucho más fuerte respecto a su peso que el kevlar, pero no doscientas veces más fuerte.

Esos materiales existen. Las fibras de carbono microscópicas parecen tener las propiedades necesarias. Así que, de acuerdo con cálculos teoréticos, servirían los nanotubos, largas fibras de átomos de carbono unidas las unas a las otras. Tampoco se encuentra ahora en producción industrial con los tamaños necesarios, pero eso podría cambiar en el futuro muy cercano.

Una buena característica del carbono, aparte de su capacidad para hacer materiales muy fuertes, es que algunos asteroides están hechos en

gran parte de ellos. Se mueve uno de ellos en órbita y se equipa con una industria capaz de convertir carbono en cable extrafuerte. Cuando se haga, se usa lo que sobra del asteroide como contrapeso, se une al cable que sale del satélite y se aleja de la Tierra, lo que permite sostener el cable inferior con un cable superior mucho más pequeño. Nadie pujaría por el proyecto ahora mismo, pero en principio es factible.[172]

Y ahí vamos

Piensa en un contenedor de carga levantando el cable. Abajo, sus motores tienen que elevar todo su peso. A medida que va estando más alto, la gravedad se hace más débil, la fuerza centrífuga es más fuerte, así que se vuelve cada vez más fácil levantarlo. Cuando llega al satélite en órbita geosincrona, los dos se equilibran de forma exacta; dentro del contenedor, flotas. Deja que el contenedor continúe subiendo, siguiendo el cable superior hasta el espacio. Ahora la fuerza centrífuga sobrepasa la gravedad. Sin motor ni frenos, vas cada vez más rápido.

Una posibilidad es usar ese proceso, calculando cuidadosamente el tiempo, para lanzarte al espacio. En principio, sería posible construir ascensores espaciales en una serie de planetas diferentes y usarlos para el transporte interplanetario en vez de cohetes. Piensa en ello como un gigantesco juego de coger la bola. Se te lanza desde la Tierra soltando el ascensor espacial en el momento y lugar apropiados. Cuando te aproximes a Marte, ajustas un poco tu trayectoria (probablemente seguirás necesitando cohetes para poner a punto el sistema), de forma que las velocidades concuerden con el ascensor espacial que orbite alrededor de Marte. Sal de ese en el tiempo adecuado, tras acercarte o alejarte una distancia apropiada, y te encuentras de camino al cinturón de asteroides, o quizás a Júpiter. Construir un ascensor espacial en

---

[172] Aun sonando a especulación salvaje, la idea de usar nanotubos para sujetar un ascensor espacial la propuso de forma seria Richard Smalley, de la Universidad de Rice, al que se le otorgó en 1996 el Premio Nobel de Química por su descubrimiento de los fulerenos, la familia de moléculas de carbono a la que pertenecen los nanotubos. Se pueden encontrar imágenes de una gran variedad de fullerenos en http://cnst.rice.edu/pics.html. Hay un artículo optimista acerca de usar nanotubos de carbono para construir un ascensor espacial, quizás tan pronto como en 2017, en http://www.sciencenews.org/20021005/bob9.asp.

Júpiter podría plantear problemas incluso para el mejor cable que la nanotecnología pueda hacer dar vueltas: quizás deberíamos usar uno de sus satélites en su lugar. Es una idea que marea.

Una alternativa es equipar la cápsula de cargamento con frenos regenerativos, una idea que ya se ha implementado en coches eléctricos e híbridos. Un freno regenerativo es un generador eléctrico que convierte la energía cinética de un coche en electricidad, parando el coche y recargando sus baterías. En el ascensor del espacio, la electricidad generada por los frenos que evitan que una cápsula de cargamento despegue hacia Marte se podría usar para elevar el siguiente de la Tierra al satélite.

Los lectores escépticos podrían preguntarse de dónde viene esa energía usada para lanzar naves espaciales alrededor del sistema solar o elevar cápsulas desde la Tierra. La respuesta es que proviene de la rotación terrestre. Cada vez que elevas una carga por el ascensor, se está acelerando en dirección a la rotación terrestre, puesto que cuanto más alto, más rápido tiene que moverse para dar una vuelta diaria a la Tierra. Por cada acción hay una reacción; la conservación del momento angular implica que acelerar la carga frena la Tierra. Por suerte, la Tierra es mucho más grande que nosotros o que las cosas que subamos por el ascensor, así que llevaría mucho tiempo hasta que el efecto se volviera significativo.[173]

No he intentado calcular cuánta masa se podría mandar al espacio antes de que los astrónomos se quejaran de que los relojes atómicos iban deprisa.

Arthur C. Clarke

El ascensor espacial que he descrito no se puede construir con materiales que estén disponibles actualmente. Pero hay al menos dos versiones modificadas del diseño que quizás puedan. Una se llama *skyhook* o gancho celeste. Lo propuso Hans Moravec en Estados

---

[173] La posibilidad de extraer la energía rotacional sugiere una idea de ciencia ficción interesante: una expedición interestelar descubre un sistema planetario en el que ninguno de los planetas están rotando porque sus ciudadanos usaron toda su energía rotacional, punto en el que su civilización interplanetaria, basada en el transporte usando esa energía, colapsó.

Unidos en 1977, pero Artsutanov había publicado la idea en 1969. He aquí cómo funciona.

Comienza, en esta ocasión, con un satélite mucho más cercano a la Tierra. De nuevo se sueltan dos cables, uno arriba, otro abajo. Ya que este satélite no se encuentra en órbita geosincrona, se está moviendo en relación a la superficie de la Tierra. Esto hace difícil unir la parte inferior del cable a nada, así que no lo hacemos. En lugar de ello, rotamos el cable, un extremo bajo el satélite, otro por encima, como dos radios de una rueda gigantesca que da vueltas alrededor de la Tierra.

El satélite se está moviendo alrededor del globo, pero el extremo de abajo del cable, cuando está en su punto más bajo, está estático; el movimiento del cable relativo al satélite cancela el movimiento del satélite relativo a la Tierra. Si esto suena raro, piensa en un coche yendo por la autopista a 95 kilómetros por hora. El coche se está moviendo, pero la parte de abajo del neumático está quieta, ya que la rotación de la rueda lo mueve hacia atrás en relación al coche tan rápido como el coche se mueve hacia delante en relación al pavimento. El gancho celeste aplica el mismo principio a mayor escala.

Visto desde la Tierra, el extremo del cable baja desde el espacio, se para en la parte inferior de su trayectoria, sube de nuevo. Para usarlo para el transporte espacial, pones la cápsula de cargamento en un avión, la transportas hasta donde va a estar el cable, lo enganchas justo cuando la parte de abajo del cable alcance su punto más bajo. La ventaja sobre el ascensor espacial es que la órbita mucho más baja significa un cable mucho más corto, así que se puede estar mucho más cerca de construirlo con materiales que estén disponibles actualmente. La física funciona, pero no esperes que la Junta Aeronáutica Civil dé el visto bueno a llevar pasajeros en poco tiempo.

Una versión diferente que podría funcionar incluso antes la propusieron investigadores del proyecto de investigación avanzado Skunk Works, de Lockheed Martin, fuente de gran parte de la innovación aeronáutica del pasado. Comienza con una simple observación: poner algo en órbita es mucho más de dos veces más difícil que ponerlo a medio camino de la órbita. Si tienes dos

tecnologías completamente distintas para ponerlo en órbita, ¿por qué no dejar que cada una de ellas haga la mitad del trabajo?

La propuesta de Skunk Works usa un pequeño gancho espacio, que alcanza desde un satélite en una órbita baja y baja hasta un punto por debajo de la atmósfera. Lo combina con una nave espacial, un cruce entre un avión y la lanzadera espacial, capaz de despegar desde un aeropuerto ordinario y levantar su carga gran parte del camino, pero no todo, hacia la órbita. SpaceShipOne, el innovador vehículo de Burt Rutan que hace poco ganó el premio Ansari X PRIZE, de diez millones de dólares, proporciona una prueba del concepto, aunque su capacidad de carga es un poco baja. La nave espacial lleva la cápsula de cargamento hasta el gancho celeste; este la lleva el resto del camino. Los ingenieros a los que se les ocurrió el diseño creen que se podría construir hoy y que reduciría el coste de elevar material al espacio hasta los quinientos cincuenta dólares por kilo y medio. Eso es mucho más que el coste estimado con un ascensor espacial, pero es alrededor de una décima parte del coste de usar un cohete.

CONCENTRANDO LA MENTE: EL PROBLEMA DE LOS OBJETOS CERCANOS A LA TIERRA

Nada concentra tanto la mente de un hombre como las perspectivas de que se le cuelgue por la mañana.

Samuel Johnson

Hace un poco menos de un siglo (en 1908), Rusia sufrió una detonación aérea de quince megatones. Por suerte, el objetivo no fue Moscú, sino un pantano siberiano. La explosión derribó los árboles de un área de unos mil seiscientos kilómetros cuadrados. Mientras que todavía hay cierta incertidumbre sobre lo que fue el suceso de Tunguska, la mayor parte de los investigadores están de acuerdo en que fue algo del espacio, quizás un meteorito pequeño o parte de un cometa, que impactó en la Tierra. Se estima que su diámetro era de aproximadamente sesenta metros. Mientras que es el suceso de este tipo más grande en la historia registrada, hay pruebas geológicas de

impactos mucho más grandes. Uno, que ocurrió hace unos sesenta y cinco millones de años, dejó un cráter de ciento ochenta kilómetros de largo y es una explicación posible para el periodo de extinción masiva que eliminó a los dinosaurios.

2002 CU11 es un objeto cercano a la Tierra, un asteroide en una órbita que se acercará a la Tierra. Su diámetro estimado es de setecientos treinta metros. Ya que el volumen es el cubo del diámetro, esto significa que probablemente tiene más de mil veces la masa del meteoro de Tunguska y podría hacer mucho más daño en comparación, mucho más que la bomba H más grande que jamás se haya probado. Poco después de que se avistara por primera vez, se estimó que 2002 CU11 tenía una posibilidad entre nueve mil de impactar con la Tierra en 2049. Te aliviará saber que observaciones posteriores, que permitieron un cálculo más preciso de su órbita, han reducido esa probabilidad a prácticamente cero.

2000 SG344 es una roca mucho menor, de unos cuarenta metros. La NASA estima que tiene una posibilidad entre quinientas de impactar contra la Tierra en algún momento entre el 2068 y 2101. Incluso una roca tan pequeña produciría una explosión mucho más potente que la bomba que se soltó en Hiroshima.

Según estimaciones actuales, hay unos mil objetos cercanos a la Tierra de un kilómetro de diámetro o más y un número mucho más grande de menores. Pensamos que hemos visto más de la mitad de los grandes; ninguno parece seguir un rumbo que pueda provocar colisión. Puesto que un objeto que pasará junto a la Tierra en algún punto de su órbita podría estar a mucha distancia en ese momento, localizar todos ellos es difícil.

Nuestro mejor supuesto por el momento, a partir de las pruebas geológicas, es que los asteroides realmente grandes (de dos kilómetros y superiores) impactan sobre la Tierra en una relación de uno o dos cada millón de años. Eso hace que las probabilidades de que tenga lugar durante la vida de una persona sean de más o menos una entre diez mil. Los impactos mayores son mucho más comunes: uno que llegue al megatón en el último siglo.

Las probabilidades de un gran impacto son bajas, pero, dado el daño que podría hacer, es algo de lo que merece la pena preocuparse. Las

probabilidades de un pequeño impacto, que podría hacer un daño significativo si llegara a impactar en una zona poblada o en el mar cerca de una costa poblada son mayores. ¿Qué podemos hacer?

El primer paso es vigilar las cosas que se dirijan hacia nosotros. La NASA, junto con investigadores de otros países, ha estado trabajando en ello; por eso puedo citar tamaños y probabilidades de los objetos cercanos a la Tierra conocidos. La congresista Dana Rohrabacher ha propuesto unir eso con una solución más centralizada: premios económicos para recompensar a los astrónomos aficionados que avisten asteroides cercanos a la Tierra que no se conocían previamente. Ya que los objetos se están moviendo en órbitas determinadas por las leyes de la física, una vez hayamos avistado uno de ellos varias veces, podemos realizar una proyección bastante precisa de dónde estará a lo largo de varios años. Se espera que un asteroide particularmente bien observado,[174] de un poco más de un kilómetro de diámetro, realice un pequeño acercamiento a la Tierra el 16 de marzo del año 2880.

Supón que avistamos un asteroide de camino a la Tierra. Si va a impactar mañana, no hay mucho que se pueda hacer más que ir tan lejos como sea posible del punto de impacto y muy por encima del nivel del mar. Pero si lo avistamos lo bastante pronto, podríamos ser capaces de evitar la colisión. Mover un asteroide grande es difícil, pero mediante una década o más de empujar con una pequeña fuerza se puede modificar su órbita al menos un poco. Incluso un pequeño cambio en la órbita, actuando durante mucho tiempo, puede convertir un impacto en nada.

Una solución sería aterrizar en el asteroide, equipados con un pequeño reactor nuclear, usarlo para vaporizar la roca y explotarlo frente al espacio, moviéndolo ligeramente hacia la otra dirección. Una solución menos elegante, pero que usa el *hardware* convencional que ahora está disponible con exceso de suministros, es bombardearlo atómicamente. Explota una bomba nuclear o termonuclear sobre, ligeramente por debajo o ligeramente por encima de la superficie del asteroide. Explotada bajo la superficie, vuela trozos del asteroide (con suerte, trozos lo bastante pequeños para que no sean ellos mismos demasiado peligrosos) en una dirección y desplaza el resto del asteroide

[174] 1950 DA.

hacia la otra. Sobre o cerca de la superficie, vaporiza parte de la superficie y lo conduce en una dirección, dando al asteroide un breve pero fuerte empujón hacia el otro lado. Para un asteroide con un diámetro de un kilómetro o así avistado una década o más antes de que nos impacte, una solución así podría valer.

Las probabilidades de un impacto catastrófico de un asteroide son bajas, pero el riesgo podría ser sustancial. Si los dinosaurios hubieran tenido un programa espacial adecuado, todavía podrían seguir por aquí.

AD ASTRA

Actualmente estamos activos en el patio trasero de la Tierra, montando satélites de comunicaciones, espías en el cielo y cosas similares. He sugerido algunas posibilidades para el siguiente paso: reducir el coste de salir de la Tierra lo bastante para hacer posible establecer poblaciones humanas sustanciales en hábitats espaciales o asteroides modificados adecuadamente. El paso siguiente es mucho más difícil, porque las estrellas se encuentran mucho más lejos. La física actual sostiene que nada se puede mover más rápido que la velocidad de la luz. Si esto sigue siendo cierto, los viajes a otras estrellas llevarán años, probablemente décadas, posiblemente siglos. Podríamos comenzar a pensar en ellos ahora mismo.[175]

Los capítulos anteriores proporcionan tres soluciones para el problema de mantener viva a la tripulación de una expedición interestelar lo bastante para llegar a algún sitio. Una es alargar la vida. Otra es la suspensión criónica. Una tercera es que la nave esté tripulada por ordenadores programados. Si un programa se aburre, se puede guardar a sí mismo en el disco duro, o el equivalente que haya por entonces, y desconectarse. Tras, por supuesto, recordar a otra IA que lo recargue cuando lleguen.

¿Y la propulsión? Hacer que una nave espacial viaje a una fracción significativa de la velocidad de la luz requiere algo considerablemente

[175] En esta sección estoy, hasta cierto punto, violando mi norma de discutir solo las décadas inmediatamente próximas. A pesar de que podríamos lanzar nuestra primera nave interplanetaria tan pronto, es muy improbable que lleguemos a otra estrella antes de que el margen de tiempo que me he impuesto haya pasado.

mejor que los cohetes químicos. Se han hecho y analizado una serie de propuestas. Una de mis favoritas comienza con una forma de propulsión propuesta algunas décadas atrás para el vuelo interplanetario y con la que actualmente se está experimentando: velas. No hay aire en el vacío el espacio, pero hay mucha luz, y la luz tiene presión. Una vela ligera es una fina película de material reflectante con un área de muchos kilómetros cuadrados, quizás muchos miles de kilómetros cuadrados. La nave unida a la vela controla su ángulo con el Sol, como se controla una vela ordinaria controlada en la Tierra.

La luz solar va toda en una dirección: hacia fuera. Su presión se puede usar para conseguir aceleración en dirección contraria al Sol, pero ¿cómo volver? Una respuesta es mediante gravedad. Así como un barco de vela ordinario combina la presión de su quilla contra el agua con la presión del viento contra la vela, una nave solar combina la presión de la luz con el empuje de la gravedad solar. Para acelerar en ángulos correctos hacia la dirección del Sol, se inclina la vela de tal forma que la combinación de la presión de la luz y la gravedad se sumen al vector que se desee. Para acelerar en dirección al Sol, se recoge la vela o se inclina de forma que el borde quede en dirección hacia la luz, y se espera a que el Sol te atraiga.

La gran ventaja de una vela de luz es que no necesita combustible. Un problema es que cuanto más lejos estés del Sol, menos hay para que te impulse; para un viaje interestelar, el Sol es solo una estrella. La solución es proporcionarte tu propia luz solar. Se construye un láser muy poderoso en alguna parte del sistema solar, se apunta a la vela de la nave interestelar y se la empuja por el espacio. La nave marcha: la fuente de energía se queda detrás.

Una vela solar apoyada por un cañón láser muy grande es una solución elegante para el problema de llegar a las estrellas, pero sigue quedando un problema: parar. A menos que la estrella a la que vayas también esté equipada con un cañón láser, estás tripulando una nave sin frenos.

Mi solución favorita la ofreció Robert Forward. Su barco tiene dos velas solares, un círculo dentro de otro más grande. Cuando te acercas al sistema que desees, te desprendes del anillo externo y ladeas todo de forma que el rayo láser no dé en la vela que aún está unida a la nave,

impacte en la otra, rebote y se reflecte en la primera. La vela desprendida se acelera hacia el espacio, dirigida por el rayo, mientras que la nave se va frenando por el rayo reflejado que impacta en la vela que todavía está unida.

Antes de que llegue la segunda nave, la primera construye un segundo cañón láser para proporcionar frenos. Nadie podría esperar que una maniobra tan complicada funcionara dos veces. Una vez tienes un láser en cada extremo, se vuelve mucho más fácil el viaje de ida y vuelta.

The sunside armor’s peelin’, and the reels have too much slack,
And it takes a week to get her up to speed.
The mainsail’s full of pinholes, and the coffeemaker’s cracked,
But I can’t think of anything I need.
As twelve hundred klicks of sail begin to furl, and keel jets hiss,
And the pickup point sends grapnels out to roam,
I fin’ly have the chance to think of one I love and miss,
Running down the windward passage to our home.
Running down the windward passage to our home.
You’ll never call me wealthy, and I haven’t come too far,
And there’s folks I know would make me out a fool.
But they’ve never cruised the system, and they’ve never sailed the stars,
With ten million miles of sunlight for their fuel.

WINDWARD PASSAGE
Letra y música de Michael Longcor, 1989

P.O. Box 30268, Portland, OR 97294
Firebirdarts.com

CINCUENTA AÑOS DESPUÉS DE QUE DEJEN DE REÍRSE

¿Qué probabilidad hay de que suceda cualquiera de estas cosas? La nanotecnología haría técnicamente posible un ascensor espacial, pero

todavía habría problemas políticos para construir un proyecto de esa escala. Si se demostrará que son insuperables o no depende del clima de la opinión dentro de treinta o cuarenta años, lo que es difícil de predecir. Incluso sin un ascensor espacial, la nanotecnología debería hacer posibles materiales mucho más fuertes y ligeros, lo que reduciría de forma increíble los costes de lanzamiento, quizás lo suficiente para establecer una presencia humana real en el espacio. La defensa contra los objetos cercanos a la Tierra es una de las razones para hacerlo, una razón que podría volverse urgente si avistáramos algo grande en camino a una colisión.

El viaje interestelar es un proyecto más difícil. Podría suceder, y es interesante pensar en ello, pero no espero que nadie llegue a otra estrella en algún momento de los últimos cincuenta años, un punto tan lejano que no tenemos ninguna esperanza razonable de predecir la tecnología futura. Si llega a suceder, el magnífico apaño de Forward, la vela dentro de una vela, es tan probable como cualquier otra cosa.

Adaptaré la respuesta que me dio Arthur Kantrowitz cuando alguien planteó una pregunta parecida sobre sus sistemas de propulsión láser. El Ascensor Espacial se construirá unos cincuenta años después de que todos dejen de reírse.

Arthur C. Clarke

VEINTIDÓS

TIEMPOS INTERESANTES

Que vivas en tiempos interesantes.

Antigua maldición china, aparentemente inventada por Eric Frank Russell alrededor de 1950.

FUTUROS MÚLTIPLES

Un escritor que mirara hacia el futuro en 1900 podría haber anticipado los cohetes. Podría haber anticipado los explosivos nucleares. El balance nuclear del terror, uno de los hechos centrales de la segunda mitad de siglo, requería ambos. A lo largo de la mayor parte de este libro, he tomado los futuros de uno de uno. No vendrán de esa manera.

Ya se discutió una interacción entre tecnologías en el capítulo 5. Si el ciberespacio es privado y el espacio real, público, cuánta privacidad tengamos depende de cuánta parte de nuestras vidas vivamos en cada uno. En cambio, eso depende de otra tecnología: la realidad virtual. En el límite de la realidad virtual profunda, todo lo importante sucede en el ciberespacio, dejando poco que ver a las cámaras automatizadas de la sociedad transparente.

Otro ejemplo apareció en el capítulo 21. La importancia del papel que representa el espacio en nuestras vidas durante el próximo siglo depende de lo caro que resulte llegar ahí. Eso, en cambio, depende de la relación fuerza-peso de los materiales disponibles. Con materiales lo bastante fuertes y ligeros, se vuelve posible construir un ascensor espacial, lo que reduciría drásticamente el coste de salir de la Tierra. Además, los materiales de mejor calidad hacen posibles los vehículos de lanzamiento con una carga mucho más grande y costes mucho menores. Una forma de obtener materiales muy fuertes y pesados, como las fibras de carbono de una molécula, es la nanotecnología.

En algunos casos, una tecnología elimina problemas planteados por otra. Las pruebas genéticas hacen que no se puedan asegurar los riesgos genéticos. Pero con una ingeniería genética lo bastante avanzada, eso no importa, ya que no quedarán riesgos genéticos que asegurar. Las tecnologías de identificación biométrica pueden imponer sobre todos un carnet de identidad incorporado infalsificable (hasta que la nanotecnología haga posible, incluso sencillo, revisar las huellas dactilares o el patrón del vaso sanguíneo de la retina). La suspensión criogénica plantea rompecabezas conectados con castigar adecuadamente a los delincuentes que elijan congelarse mientras que sigue corriendo su condena, pero si la tecnología de vigilancia produce un mundo en que los delincuentes se enfrenten a una certeza de condena próxima, el castigo adecuado podría no ser un problema. Si sabemos lo bastante sobre cómo funciona un cerebro humano para imitarlo en silicio, podríamos saber lo bastante para rehabilitar a delincuentes mediante métodos menos rudimentarios que la prisión. Por supuesto, ese conocimiento, y ese poder, podrían crear otros problemas que es posible que hagan parecer insignificantes los problemas de crimen y castigo.

IMPERFECTO FUTURO

En los anteriores veintiún capítulos hemos pensado en una amplia variedad de futuros posibles, algunos atractivos, otros aterradores, pocos insípidos. La mayoría ofrecen tanto problemas como promesas. Evitando lo primero tanto como sea posible y aprovechando lo último, podemos, en la mayoría de los casos, estar mejor que si la tecnología no existiera. Pensemos en unos pocos ejemplos.

La encriptación, el dinero electrónico y las redes informáticas disponibles globalmente harán más sencillos ciertos delitos; harán más sencillo, por ejemplo, recoger el rescate del secuestro o extorsión sin ser cogido durante el proceso. Pero esas tecnologías también proporcionan nuevas y poderosas maneras de protegernos a nosotros mismos del delito. También hacen mucho más difícil que los Gobiernos controlen a la gente. Los Gobiernos, según las pruebas históricas, son mucho más

peligrosos que los delincuentes privados; durante el último siglo, los Gobiernos mataron a más de doscientos millones de las personas a las que gobiernan, excluyendo las guerras.[176] Según mi visión, al menos, los beneficios de debilitar el poder de los Gobiernos son mucho más grandes que los costes.

La tecnología reproductiva humana, la capacidad de los padres para elegir cuáles de los niños que podrían tener tendrán o usar la ingeniería genética para proporcionar a los niños características que la naturaleza no consiguió darles plantea problemas potenciales, ya que las decisiones importantes las tomará la gente antes de que nazcan, y será necesariamente otra gente la que las tome. Pero esas elecciones no son diferentes de las que ya hizo otra gente para sus hijos, como la decisión de traerlo al mundo y la decisión sobre cómo criarlo o criarla.

Un Gobierno con un horizonte de tiempo lo bastante largo podría usar esas tecnologías para intentar criar a guerreros, científicos o burócratas superiores. Pero un Gobierno así podría hacer lo mismo usando técnicas de cría selectiva que hemos estado aplicando a otras especies durante varios miles de años. Pocos o ninguno lo han hecho, quizás porque los Gobiernos rara vez tienen un horizonte temporal tan largo.[177]

Estas tecnologías también podrían concedernos la capacidad, dentro de una o dos generaciones, de eliminar tanto las enfermedades genéticas como un amplio rango de otras desventajas hereditarias, como el problema de corazón que mató a mi abuelo paterno de joven, y, a una edad mucho más avanzada gracias a la medicina moderna, a mi padre. También contiene el potencial para incrementar la inteligencia media de nuestra especie, lo que podría ser una mejora y, sin duda, será interesante.

Las implicaciones de otras tecnologías son más ambiguas. Ejemplos obvios son la nanotecnología y la inteligencia artificial. Cada una podría conducir a un mundo enormemente más atractivo. Ambas

---

[176] Los números están basados en cálculos realizados por R. J. Rummel en http://www.hawaii.edu/powerkills/welcome.html y http://www.freedomsnest.com/rumrud.html.

[177] Uno podría argumentar que el sistema de funcionariado chino (exámenes abiertos a todos, dándoles a los que más puntuación obtienen posiciones públicas que llevan con ellas un estatus e ingresos en una sociedad poligenia) era un sistema de educación selectiva. No conozco ninguna prueba de que esto fuera lo que se pretendía.

contienen el potencial para desencadenar una catástrofe en una escala que no se ha visto en la Tierra desde la eliminación de los dinosaurios hace unos sesenta y cinco millones de años.

El progreso tecnológico significa que podemos hacer más cosas. Las hacemos porque creemos que realizarnas nos beneficia, por lo que uno podría esperar que siempre estuviéramos mejor con tecnologías nuevas que sin ellas. Si hay excepciones para esa conclusión, ¿por qué? ¿Hay alguna lógica mediante la cual, en algunos futuros posibles, el progreso tecnológico pudiera hacernos estar peor?

La hay. El primer paso hacia su comprensión es pensar un poco más cuidadosamente en el mundo imposible en el que vivimos ahora, en cómo funciona y cómo podría dejar de funcionar.

EL PROBLEMA DE COORDINACIÓN

Nuestro mundo se encuentra poblado por un gran número de individuos. Cada uno tiene sus propios objetivos, creencias y habilidades. Para que funcione una sociedad moderadamente complicada, esos individuos deben encontrar alguna forma de coordinar sus esfuerzos. Para que yo construya una espada o un arado, alguien tiene que fundir hierro. Para que aquel funda hierro, alguien tiene que extraer menas de hierro y producir carbón vegetal. Cada uno de ellos necesita los resultados producidos por otras actividades llevadas a cabo por otra gente. Y una vez tenemos un arado, de poco sirve si no hay un agricultor para arar la tierra, semillas para plantar y mucho más.

En una sociedad moderna, el problema es todavía más difícil. Para un ejemplo que no es mío[178], piensa en un lápiz. La madera de la que está hecho requiere, yendo atrás en la cadena, árboles y aserraderos y sierras continuas y gasolina y baterías y hierro y generadores eléctricos y altos hornos y mena de metal y carbón y... Sigue todas las líneas y tienes millones de personas coordinando sus actividades para producir un lápiz, una camisa, un ordenador.

---

[178] Léase 1958. En http://www.fee.org/pdf/books/I,%20Pencil%202006.pdf.

¿Cómo podemos hacerlo? ¿Cómo podemos asegurarnos de que la mina produzca la cantidad de mena necesaria para hacer la cantidad de hierro necesaria para...? ¿Cómo podemos resolver ese problema un millón de vez, cuando cada pieza depende de cada otra pieza?

Solo hay dos soluciones conocidas, y una de ellas no funciona. Esa, la obvia, es el control central. Alguien tiene el trabajo de descubrir lo que todos los demás deberían hacer, decirles qué hacer y asegurarse de que obedezcan. En una escala familiar, una empresa, un equipo de fútbol, podría llegar casi a funcionar, aunque incluso ahí es probable que un examen cuidadoso encuentre que la gente hace muchas cosas que se les ha dicho que no hagan. Pero la eficacia de la solución centralizada no aumenta progresivamente. A medida que la empresa se vuelve más grande, cada vez tiene que pasar más información por la autoridad central, la mayor parte de la cual va perdiéndose en el camino, y el problema de dar con lo que todos deberían hacer se vuelve complicado hasta el punto de no funcionar.

La solución que sí funciona (más importante, cuya eficacia aumenta de forma progresiva) es la descentralizada. Todo pertenece a alguien. La gente es libre de comerciar. Si el valor de lo que posees (incluyendo, lo que es más importante, el uso de tu cuerpo para hacer cosas que sabes cómo realizar) vale más para mí que para ti, hay alguna oferta que puedo proponer que aceptarás. Cada uno de nosotros tiene fines distintos. Pero cada uno puede ofrecer, a través de un intercambio de bienes, servicios o dinero, su ayuda para que se consigan los bienes de otra persona a cambio de que esa persona eche una mano con los suyos. Entrar en toda la lógica de este sistema requiere algo así como un semestre de teoría de precios, pero la lógica básica es muy sencilla.

La solución descentralizada funciona mejor si hay alguna definición de los derechos de propiedad, alguna forma de dividir el mundo en trozos, de forma tal que el uso que cada individuo haga del suyo tenga efectos significativos solo sobre sí mismo y poca gente más (idealmente, efectos que ocurran solamente con el consentimiento mutuo de ambas partes). Mi uso de la habilidad para contar historias solo me afecta a mí y a aquellos que elijan escucharlas; si no me ofreces términos aceptables, no elegiré contarte historias. Algo parecido con la mayoría de bienes o servicios. Siempre que se cumpla esa condición, cada uno

de nosotros puede decidir qué hacer en términos de su valor para él (me gusta contar historias) y su valor para otra gente, medido por lo que estén dispuestos a ofrecerle a cambio.

Por desgracia, en cualquier mundo razonablemente complicado, no hay una definición de derechos de propiedad que cumpla por completo esta condición. Que yo cuente mi historia es una interacción voluntaria entre mí mismo y la audiencia que quiere escucharme, pero cuando llego a las partes más ruidosas se vuelve una interacción involuntaria entre mí y mi vecino. Que yo conduzca un coche es el resultado de comerciar voluntariamente con la gente que construyó el coche, refinó la gasolina, vendió los mapas. Pero impone costes de forma involuntaria sobre la gente a la que podría atropellar y los que respiren los gases del tubo de escape.

En los casos más simples, cuando estos costes externos se vuelven significativos, podemos lidiar con ellos (y lo hacemos) mediante el derecho de responsabilidad civil. Si hago ruido demasiado tarde por la noche, mi vecino podría ser capaz de obtener un auto preventivo. Si conduzco negligentemente y mi coche acaba en tu salón, te deberé un pago por el daño hecho. El litigio es un mecanismo más torpe y menos eficiente que el comercio; como media, de cada dólar que gasta un acusado, solo cincuenta céntimos acaban yendo al demandante; el resto va a los abogados, costes del tribunal y similares.[179] Pero sí proporciona un mecanismo para forzar a los individuos a preocuparse por los costes que imponen sobre los otros cuando deciden qué hacer con su propiedad.

A medida que los efectos se vuelven más dispersos (no un gran daño a una persona por cuya casa pasé con el coche, sino un daño pequeño a cada una de los diez millones de personas con la mala suerte de estar respirando mis gases de escape), el derecho de responsabilidad civil se vuelve cada vez menos útil. El daño de un contaminante particular es, en la mayoría de los casos, difícil o imposible de medir. Aunque existen mecanismos legales como la demanda general, diseñados para combinar grandes números de víctimas en una por fines de litigio, funcionan muy mal. En estos casos, la respuesta típica es aguantar el problema o intentar resolverlo mediante regulación gubernamental.

---

[179] Una antigua estimación de Viscusi, 1991.

La regulación gubernamental es una vuelta a la solución centralizada, alguien de arriba decidiendo lo que el resto debería hacer y encargarse de que lo hagan. Por razones sugeridas antes y exploradas en otra parte con mayor detalle por mí y por otros,[180] funciona muy mal, especialmente cuando se aplica a grandes sociedades. Nosotros no tenemos ninguna forma de hacer que las agencias reguladoras intenten actuar en nuestro interés y ellas no tienen ninguna manera buena de dar con cómo hacerlo.

Cuando la escala del efecto se vuelve internacional, el problema empeora. Las agencias reguladoras del Gobierno de EE.UU., como la FDA (Agencia de Medicamentos y Alimentos) o la FCC (Comisión Federal de Comunicaciones) pueden tener intereses políticos, ser incompetente o ambas, pero al menos poseen algún interés por hacer cosas que los ciudadanos estadounidenses aprueben. Gozan de muy pocas razones para que les importe el efecto de sus políticas sobre los ciudadanos de Bangladesh o las Islas Maldivas.

Para un ejemplo del tipo de problema que no se puede confiar en que resuelvan las soluciones centralizadas ni las descentralizadas, pensemos en el cambio climático debido a actividades humanas. Aunque hay mucha discrepancia legítima sobre su escala y consecuencias probables, hay muchas razones para creer que existe y que se debe al menos en parte a los incrementos en la cantidad de dióxido de carbono en la atmósfera.

Cuando uso electricidad generada por quemar carbón, o enciendo un fuego en mi chimenea, o respiro, estoy produciendo dióxido de carbono (CO_2). Un resultado de esto es un diminuto incremento en la temperatura de la Tierra. Una consecuencia de eso podría ser un incremento muy pequeño en el nivel del mar. Los efectos predichos, incluso tras combinar las implicaciones de la actividad de todo el mundo, no son muy grandes: las estimaciones actuales[181] sugieren un

---

[180] Friedman, 2000, p. 30. Véase también Buchanan y Tullock, 1962, Mueller, 2003, y otras obras de elección pública.

[181] El sitio de IPCC es http://www.ipcc.ch/. El informe de 2007 se encuentra en http://www.ipcc.ch/ipccreports/ar4-wg2.htm. El tope del rango del aumento del nivel del mar que aparecía en el informe de 2001 era de 80 centímetros. El de 2007 presenta una variedad de posibilidades: predice aumentos que van desde 0,18 a 0,59 metros mientras que se niega a describir ninguno de ellos como un máximo, y menciona la posibilidad de aumentos mucho mayores a lo largo de periodos de miles de años y la incapacidad de estar seguros de que

incremento de temperatura de unos dos grados centígrados y un aumento de medio metro o menos durante el próximo siglo. Donde vivo, en la Costa Oeste de EE.UU., eso será un inconveniente menor: las playas serán un poco más estrechas. Será más problemático para la gente que viva en territorios bajos bajo la amenaza constante de inundaciones. Y si resulta que la tasa del calentamiento global y el cambio en el nivel del mar son sustancialmente mayores que lo que sugieren las estimaciones presentes, podría ser, sin duda, un problema muy serio.

¿Cómo podríamos lidiar con ese problema? No podemos definir muy bien los derechos de propiedad de una forma que proporcione a cada habitante de Bangladesh un veto sobre el uso de potencia, calentamiento del hogar y respiración de cada estadounidense. No podemos esperar que el sistema legal internacional honre y ejecute las demandas civiles de un ciudadano de Bangladesh contra uno de EE.UU. por contribuir con una parte de diez mil millones a una inundación de dentro de cincuenta años. Podríamos imaginarnos al Gobierno de Bangladesh intentando usar la ley internacional para forzar al Gobierno de Estados Unidos a regular con firmeza las actividades de sus propios ciudadanos que se predice que incrementarán el riesgo de futuras inundaciones en Bangladesh, pero, si las regulaciones son costosas para los estadounidenses, ¿por qué debería cumplirlas el Gobierno de EE.UU?

Podemos imaginarnos, y, por supuesto, hemos observado intentos de negociar tratados internacionales para el mismo propósito. Pero mientras que los argumentos acerca del cambio climático a veces podrían ser útiles para ayudar a los Gobiernos a persuadir a sus ciudadanos a soportar acciones que los Gobiernos ya favorecen (digamos, impuestos energéticos adicionales deseados como una fuente de ingresos y que pueden defenderse como formas de contener el consumo energético y, por tanto, la producción de CO_2), es difícil ver

---

estos incrementos no ocurrirán a lo largo de siglos. Para una crítica de la visión del cambio climático como una catástrofe masiva que debe pararse, véase http://www.cato.org/pub display.php?pub id=9125. Sin embargo, se han propuesto situaciones más drásticas que podrían llevar a incrementos mucho más grandes en los niveles mundiales del mar, algunos provocando el colapso de la capa de hielo antártica. Véase, por ejemplo: http://www.abc.net.au/7.30/content/2007/s1870955.htm.

que hagan mucho más que eso. Los Estados Unidos, al controlar las actividades de sus ciudadanos para evitar costes impuestos sobre los ciudadanos del resto del mundo, se encuentra en la misma situación que yo al bajar el volumen cuando molesta a mis vecinos. A falta de un Gobierno mundial, no hay un mecanismo legal análogo al derecho de responsabilidad civil para obligar a que lo hagan. Y un Gobierno mundial, al menos desde mi punto de vista, es un remedio mucho peor que la enfermedad.

El lado oscuro de la fuerza

He discutido el caso del calentamiento global no porque piense que es una amenaza particularmente seria (por razones a las que volveré pronto pienso que probablemente no lo sea, al menos en los próximos cincuenta años o así), sino porque es un problema con el que la mayoría de mis lectores estará familiarizado y cuya naturaleza es muy fácil de explicar.

El problema general del que este es un ejemplo es la caída de las condiciones que hacen posible la solución descentralizada para el problema de la coordinación. El progreso tecnológico incrementa nuestra capacidad para realizar cosas. A menudo, aunque no siempre, esto significa incrementar la escala y rango de los efectos de la acción humana. A medida que aumentan la escala y el rango, se vuelve cada vez más difícil definir los derechos de propiedad de una forma que satisfaga los requerimientos de la coordinación descentralizada, una forma en la que los efectos de mis acciones se encuentren en su mayoría confinados a mi propiedad y la de aquellos que han acordado permitir esas acciones. El resultado es alejarnos del único sistema viable para coordinar la acción humana (comercio y propiedad privada) y acercarnos a las alternativas menos viables del derecho de responsabilidad civil y la regulación.

A medida que la escala de los efectos se expande más allá de los límites de la nación individual, la regulación por parte de los Gobiernos nacionales se vuelve incluso menos capaz de lidiar con el problema. Se nos deja con la elección nada atractiva de o aguantar los problemas que

surjan de que los individuos ignoren los costes distantes y dispersos impuestos por sus acciones o crear un Gobierno mundial. Si elegimos lo último, nos encontramos intentando usar un mecanismo regulador centralizado para lidiar con problemas mucho más allá de la escala para la que son viables dichos mecanismos.

No todo el progreso tecnológico plantea estos asuntos. La encriptación y la realidad virtual hacen posible que las sociedades se acerquen al ideal de mercado que lo que tenemos ahora, ya que las interacciones que hacen posibles son completamente voluntarias. En la realidad virtual, el problema de la intrusión en un lugar, el problema más general de usos conflictivos, se desvanecen; cada uno de nosotros podemos disfrutar nuestra propia versión de la costa del Pacífico de California, una natural, una con los beneficios de la cultura comercial moderna. Lo mismo podríamos acabar diciendo también otras tecnologías.

La nanotecnología es un caso interesante porque sus efectos van en ambas direcciones. Por un lado, el creador de una nanomáquina que se reproducía a sí misma diseñada exitosamente para convertir toda la biosfera, con nosotros incluidos, en copias de sí misma impone costes externos mucho más grandes que cualquier nivel plausible del calentamiento global. Por otra parte, la nanotecnología defensiva lo bastante buena podría eliminar un amplio rango de problemas de externalidad actuales. No tengo que preocuparme de que mi vecino inhale su aire si mi frontera está patrullada por máquinas moleculares capaces de desmontar cualquier gas nocivo que la traspase. Ni siquiera tengo que preocuparme mucho de que la radiación penetre mi cuerpo desde su reactor nuclear experimental si mi cuerpo está patrullado por máquinas microscópicas de reparación de células capaces de reparar cualquier daño en tiempo real. Todavía tengo que preocuparme por lo que suceda si explota el reactor (incluso la maquinaria nanotécnica tiene sus límites), pero no de mucho más aparte de eso.

Deduzco que hay un problema general que podemos esperar se produzca por algunas formas de progreso tecnológico. Ocurre cuando las capacidades humanas cambian de maneras que hacen difícil definir los derechos de propiedad de una forma viable, una manera que permite que cada uno de nosotros se dedique a sus asuntos sin tener

que preocuparse demasiado por los efectos distantes sobre gente anónima y dispersa. Podemos esperar que algunas tecnologías cambien las capacidades humanas en esa dirección, y que otras tengan el efecto opuesto.

Molestias crecientes

Los problemas que he estado discutiendo se producen por una tecnología que ya está lista. Otros tipos de problemas se asocian con llegar ahí. Un ejemplo es el problema de invertir la jerarquía de edad y pericia. En una sociedad que cambia lentamente, lo que equivale a decir en casi toda la historia humana, los mayores, a pesar de que no corren tan rápido o ni siquiera piensan tan rápido como la gente más joven, saben más. Así que tiene sentido gozar de estructuras institucionales en las que, por media, la gente mayor tenga más autoridad sobre la gente más joven.

A medida que aumenta la tasa de cambio, también lo hace la tasa en la que se deprecia el crecimiento. El jefe del departamento de investigación sabe mucho más sobre válvulas de vacío que los jóvenes ingenieros cuyo trabajo supervisa, pero no están investigando sobre ellas. El juez de un caso de infringimiento de patente de *software* sabe mucho sobre la ley de patentes, pero sabe mucho menos sobre el *software* que el acusado o el demandante. Hasta cierto punto, puede confiar en el conocimiento de otra gente, como sus notarios, o volverse un experto temporal con la ayuda de informes proporcionados por ambas partes; el problema de la ignorancia judicial de la sustancia de la que se está realizando el litigio no es nuevo. Pero cuando más rápido cambia el mundo, más ignorante será probablemente la autoridad, de ahí que será más probable cometer errores serios en sus decisiones.

Uno no puede resolver el problema simplemente invirtiendo la jerarquía edad/autoridad, nombrando a estudiantes recién salidos de la facultad de Derecho jueces, contratando a los graduados más frescos de las universidades técnicas Cal Tech y Harvey Mudd para supervisar laboratorios de investigación. Los jueces tienen que saber sobre tanto la ley como el sistema legal que un abogado recién graduado no ha

aprendido aún, y gestionar un equipo de ingenieros requiere conocimiento de gestión además de conocimiento de ingeniería. Algunas de las habilidades requeridas para el trabajo se encuentran en campos de cambio lento, en los que el patrón tradicional tiene sentido; algunos, en campos de cambio rápido, donde no.

Un resultado de la situación es reforzar la tendencia natural de los empleados de ignorar o evadir las instrucciones de sus superiores. Eso, según mi punto de vista, es lo que realmente pasaba entre Randy Schwart e Intel. Schwartz creía, y probablemente tenía razón, que sabía mucho más sobre ordenadores conectados que los ejecutivos de Intel que le daban órdenes. Así que seguía sus instrucciones cuando pensaba que estaban mirando y el resto del tiempo hacía el trabajo que pensaba que debería hacerse, no de la forma que le ordenaron que lo hiciera.

La jerarquía invertida de pericia no solo anima a los empleados a creer que saben cómo hacer su trabajo mejor que los jefes a los que rinden cuentas, sino que también les anima a creer que pueden salirse con la suya diciendo «Sí, señor» y luego haciendo lo que les apetece. Ningún carroza de cuarenta y cinco va a dar con lo que están haciendo de verdad. Es una actitud especialmente probable en empleados con el modo de personalidad típica entre los brillantes jóvenes tecnófilos.

ECOLOGISMO, RECURSOS Y POR QUÉ AÚN NO DEBERÍAMOS PREOCUPARNOS DEL CAMBIO CLIMÁTICO

Este libro trata de futuros posibles, sus peligros y promesas. Durante los últimos cincuenta años la gente que se puede definir en términos generales como ecologistas ha escrito mucho sobre peligros futuros. Su visión de que el mundo se ve amenazado por la población en aumento, agotamiento de recursos naturales y la contaminación creciente ha recibido una prensa generalmente favorable y se acepta en amplios círculos, a pesar de su extraordinario registro de profecías falsas.

Hace treinta y cinco años, el popular *Limits to Growth* advertía de un futuro en el que la única forma de evitar una catástrofe era sumergirse en otra. Ese futuro ha llegado ya, y, si bien todavía hay problemas en el

mundo, es un mundo que, según estándares históricos, carece sorprendentemente del tipo de catástrofes predichas. Más o menos al mismo tiempo, Paul Ehrlich predijo que entre 1968 y 1977 habría carencias extremas de comida que tendrían por resultado la muerte de un séptimo de la población mundial. Desde el tiempo en que se publicó *The Population Bomb*hasta ahora, la tendencia de producción de comida mundial per cápita ha aumentado, no disminuido; las mismas hambrunas ocasionales de décadas recientes han sido el resultado no de una ausencia global de comida, sino de las condiciones, normalmente guerra civil, que evitaban que la comida llegara a la gente que la necesitaba. Mientras que algunos ecologistas han respondido al fracaso de sus predicciones cambiando sus visiones, algunos no lo han hecho, argumentando en lugar de ello que simplemente se habían equivocado un poco con el cálculo del tiempo.

Una razón por la que sus predicciones eran erróneas era su fracaso al tener en cuenta los principios económicos básicos. *Limits to Growth* consistía en su mayor parte en calcular las implicaciones de grandes modelos informáticos describiendo un conjunto de sistemas interactivos que se suponía que representaban el mundo. Lo que me impactó cuando leí el libro era que los autores, al hacer modelos del mundo, habían dejado fuera el papel de la racionalidad humana. Era como si intentaran predecir lo que sucedería en una autopista extrapolando los caminos que seguían los coches mientras ignoraban el hecho de que cada coche tenía un conductor con buenas razones para evitar colisionar con otros coches.

Pensemos en un simple ejemplo: agotamiento del suelo. En sus modelos, si los alimentos se volvieran escasos y caros, los agricultores intentarían producir más en la misma tierra. Hacer eso agotaría el suelo, así que la productividad futura caía. Si eso fuera cierto, Japón, donde hace mucho que los alimentos han sido caros, debería ser ya incapaz de sembrar nada; de hecho, la agricultura japonesa es extraordinariamente productiva. Cuando la comida es cara y se espera que siga siéndolo, los agricultores valoran no solo la productividad presente, sino la futura y, así, están dispuestos a pasar por muchas molestias para mantener o incrementar la fertilidad de su tierra.

Un análisis similar se aplica a otros recursos cuya distribución se maneja mediante los mecanismos ordinarios del mercado. Si las fuentes de energía son escasas, eso proporciona a los usuarios de energía un incentivo para encontrar formas de apañárselas con menos, a los productores un incentivo para encontrar nuevas formas de producir, y así con materias primas, tierras de cultivo y similares.

En un mundo de propiedad privada, el mismo argumento se aplica a la población. Cuando tengo un hijo, no llega con una demanda de su acción per cápita de los recursos mundiales bajo el brazo. Para obtener cosas (comida para comer, tierra sobre la que vivir), mi hijo, o yo, o alguien tiene que ofrecer al propietario de esos recursos algo a cambio, algo que ese propietario considere al menos valioso. Tener un hijo no hace más pobres automáticamente a los hijos de otro, el supuesto implícito de gran parte de la literatura ecologista.

Hasta ahora he estado considerando solo las interacciones entre mercados. Cuando vamos más allá, la situación se vuelve más complicada. Mi hijo podría acabar viviendo de la seguridad social, imponiendo costes a tu hijo contribuyente. Mi hijo podría, en el proceso de producir y consumir, generar contaminación que ponga peor a tu hijo. En estos casos y muchos otros, los recursos se distribuyen de otras formas que el intercambio voluntario, así que ya no hay ninguna razón para dar por hecho que las interacciones dejan a ambas partes al menos tan bien como lo estarían sin la interacción.

Antes de deducir que los opositores al crecimiento de la población tienen razón después de todo, recuerda que esos efectos pueden ir en cualquiera de los sentidos. Mi hijo podría acabar como contribuyente que mantiene a tu hijo, o compartiendo con tu hijo la carga tributaria de mantener a los hijos de otra gente. Mi hijo podría inventar la medicina que salve la vida de tu hijo. Una vez abandonamos el simple marco del intercambio voluntario, ya no podemos estar seguros de que estoy pagando todos los costes de mi decisión de tener un hijo. Pero requiere una contabilidad muy detallada, en gran parte basada en conjeturas, dar con si, en neto, la existencia de mi hijo hace que el tuyo esté mejor o peor.

Lo primero que publiqué de economía, escrito hace más de treinta años, fue un intento de responder a esa pregunta.[182] Deduje que había efectos negativos sustanciales sobre los otros en producir un hijo, había efectos sustancialmente positivos, y el tamaño de todos ellos no se podría estimar de forma lo bastante precisa para decidir cuál era mayor. Desde entonces no he visto razón alguna para cambiar esa conclusión.

El movimiento ecologista estaba y está equivocado, pero no del todo. La parte de sus predicciones que tiene que ver con bienes privados ordinarios producidos y vendidos en mercados (recursos naturales, energía, comida) es incorrecta porque ignora los mecanismos económicos que distribuyen los bienes por el espacio y tiempo.[183] Por eso Julian Simon, el crítico más visible de la posición ecologista, ganó su famosa apuesta con Paul Ehrlich sobre los precios futuros de las materias primas. Pero la parte de sus predicciones que tiene que ver con problemas como la contaminación, donde una persona impone costes sobre otros sin requerir su consentimiento, y donde podría ser posible redefinir los derechos de propiedad de cualquier forma viable para la cual no es cierto, podría ser acertada.

Lo que nos lleva de nuevo al cambio climático, la versión más nueva y aceptada de ese problema. En lo que respecta a la física, la lógica parece directa, aunque las complicaciones de los sistemas interactivos de la atmósfera, tierra y océano hacen difíciles las medidas de los cambios pasados y las predicciones de cambios futuros. La economía es igualmente directa: cuando decido si conducir, o quemar, o espirar, atiendo a los efectos sobre mí, pero no sobre ti. Si los últimos son negativos y, multiplicados por la población mundial, sustanciales, produciré dióxido de carbono incluso cuando, teniendo en cuenta los efectos sobre todos, no debería.

Sin embargo, no creo que debieramos estar realizando cosas grandes y caras en el presente para reducir nuestra emisión de dióxido de carbono. Una razón es que ese cambio no siempre es malo. Como en el

---

182 Friedman, 1972, en http://www.daviddfriedman.com/Academic/LaissezFaireInPopn/LFinPopulation.html.

183 Para más detalles sobre cómo se distribuyen los mercados a lo largo del tiempo, véase Friedman, 1996, capítulo 12, o Friedman, 1986, capítulo 12, en http://www.daviddfriedman.com/Academic/Price Theory/PThy Capítulo 12/PThy Capítulo 12.html

caso del incremento de la población, es necesario mirar tanto a los efectos positivos como a los negativos. Un ligero incremento en la temperatura global probablemente es algo malo si vives en los trópicos o en la tierra ligeramente por encima del nivel del mar. Podría ser bueno si vivieras en Siberia o Noruega. A juzgar por donde vive la mayoría de sus habitantes, Canadá tiene más de tres mil kilómetros de largo y, como media, menos de ciento sesenta kilómetros de ancho; un incremento moderado en la temperatura global podría duplicar su área real.

Temperatura aparte, un incremento en el dióxido de carbono probablemente es bueno. Después de todo, es una importante contribución a la fotosíntesis, así que de media deberíamos esperar que crecieran mejor los cultivos en una atmósfera con más cantidad de este gas.

Por tanto, aunque el calentamiento global podría hacer que estuviéramos sustancialmente peor, no es del todo claro que fuera así. La mayoría de lo que veo escrito sobre este asunto está claramente escrito por gente, en cualquiera de los lados, que sabe a qué respuesta quería llegar antes de empezar, lo que hace difícil que los lectores cuidadosos se formen una opinión segura. En tanto que pueda extraer una estimación objetiva de lo que leo, parece como si fuera probable que ocurriera el calentamiento global, pero improbable que sea catastrófico.[184]

La segunda razón por la que no creo que debieramos hacer mucho al respecto en el presente debería estar claro a partir de los primeros veinte capítulos de este libro. Si las estimaciones actuales son correctas (y podrían no serlo), los problemas sustanciales debido al calentamiento global están a décadas de nosotros. Incluso de aquí a un siglo el efecto sobre el nivel del mar, según estimaciones actuales, será un aumento de menos de un metro. Solo cuando vas más allá se vuelven realmente grandes los efectos.

Vivimos en un mundo radicalmente incierto. Es completamente posible que, de aquí a cincuenta años, ya no exista nuestra especie.

---

[184] Para más detalles sobre cómo se distribuyen los mercados a lo largo del tiempo, véase Friedman, 1996, capítulo 12, o Friedman, 1986, capítulo 12, en http://www.daviddfriedman.com/Academic/Price Theory/PThy Capítulo 12/PThy Capítulo 12.html.

También es posible que, de aquí a cincuenta años, tengamos poderes mucho mayores que ahora. Incluso si acabamos entre esos dos extremos, es altamente probable que en cincuenta o cien años estemos viviendo de forma muy distinta a ahora.

Eso podría significar una reducción drástica en el consumo de energía; puedes pasártelo muy bien con muy poca energía en un mundo de RV profunda. Podría significar un cambio hacia fuentes de energía como la nuclear o la solar que no generen gases de efecto invernadero. Podría significar un mundo con transporte espacial de bajo coste, con población que se expanda por el sistema solar. Podría significar maneras de bajo coste de reducir la absorción de calor del Sol por parte de la Tierra, como una gran serie de espejos en órbita. Aún más modesto, podría significar, según mi visión probablemente significará, un mundo lo bastante rico y con ingeniería lo bastante avanzada para hacer del dique de Bangladesh un proyecto considerablemente menos difícil que el de Países Bajo hace unos pocos siglos.

Si todo esto parece especulación inocente y que promete la luna, piensa en cuánto ha cambiado el mundo en el último siglo. Hace cien años, la medicina no curaba prácticamente nada; con raras excepciones, todo cuanto podía hacer un médico competente era decir a un paciente si debería tomarse unos días libres del trabajo o hacer un testamento. La forma usual de transporte individual era caminar, montar a caballo o en un carruaje tirado por caballos. La única forma de comunicación rápida disponible para la gente ordinaria era el telégrafo, mandar pequeños mensajes en código morse a un precio muy alto. La calculadora es un invento reciente; los únicos tipos de calculadora mecánica de uso común eran la regla de cálculo y el ábaco. La primera nave más pesada que el aire capaz de llevar a un humano había volado unos pocos años antes: durante doce segundos y cuarenta metros.

Los cambios desde entonces hasta ahora eran en gran parte cambios en la tecnología, en lo que los seres humanos sabían cómo hacer. Esos cambios continúan. Seguramente su tasa esté acelerando, a medida que los desarrollos de un campo facilitan los desarrollos de otro. Construir planes para el mundo de dentro de un siglo basándonos en la tecnología y práctica de hoy no tiene más sentido que en 1900, cuando un hombre con un ojo prudente hacia el futuro podría haberse

preocupado por evitar un colapso del sistema de transporte debido a una escasez de heno y avena.

El calentamiento global es un problema con el que necesitaremos lidiar en cierto punto, pero no un problema del que teníamos que ocuparnos ahora. No sabemos lo suficiente. Trabajar con tanta antelación significa arriesgarse a gastar recursos valiosos en solucionar problemas que se resolverán ellos mismos en algún tiempo entre ahora y entonces o, peor, gastar nuestros recursos en empujar el mundo hacia la que podría resultar ser la dirección errónea.

Necesariamente, las cifras son inciertas, pero es muy posible que en solo setenta años nuestra población sea de unos once millones, más de la mitad de los cuales serán pensionistas de anciana edad.

George Orwell, 1946, discutiendo el amenazante problema de la población decreciente británica.

En cuanto a 2006, la población del Reino Unido era de 60 587 000. La previsión actual para 2016 es de unos sesenta y cinco millones.

APÉNDICE I

Encriptación en clave pública: un ejemplo muy elemental

Imagina un mundo en el que la gente sepa cómo multiplicar números, pero no cómo dividirlos. Imagina que existe algún procedimiento matemático capaz de generar pares de números que sean inversos el uno del otro: X y 1/X. Por último, da por hecho que los mensajes que queremos encriptar son números simples.

Genero un par X, 1/X. Para encriptar el número M usando la clave X, multiplico X por M. Podríamos escribir

[M,X] = MX,

queriendo decir «El mensaje M encriptado usando la clave X es M por X.»

Supón que alguien tiene el mensaje encriptado MX y la clave X. Puesto que no sabe cómo dividir, no puede desencriptar el mensaje y descubrir cuál es el número M. Si, sin embargo, tiene la otra clave, 1/X, puede multiplicarlo por el mensaje encriptado para recuperar el M original:

MX(1/X) = M(X/X) = M

En lugar de esto, uno podría encriptar un mensaje multiplicándolo por la otra clave, 1/X, lo que nos daría

[M, 1/X] = M/X

Alguien que conoce 1/X pero no conoce X no tiene manera de desencriptar el mensaje y descubrir M. Pero alguien con X puede multiplicarlo por los mensajes encriptados y descubrir M:

(M/X) X = M

Así que, en este mundo, la multiplicación proporciona una forma primitiva de encriptación en clave pública: un mensaje encriptado al multiplicarlo por una clave puede solo desencriptarse con la otra.

La encriptación en clave pública en el mundo real depende de operaciones matemáticas que, como la multiplicación y la división en mi caso, son mucho más sencillas de hacer en una dirección que en la otra. El algoritmo RSA, por ejemplo, ahora mismo la forma más extendida de encriptación en clave pública, depende del hecho de que es sencillo generar un número elevado multiplicando varios números primos elevados, pero mucho más difícil comenzar con un número

elevado y factorizarlo para encontrar los números primos que pueden multiplicarse para obtener ese número. Las claves en un sistema así no son literalmente inversas la una de la otra, como X y 1/X, sino que son inversas funcionales, ya que una puede deshacer (desencriptar) lo que la otra hace (encriptar).

APÉNDICE II: ENCADENAR *REMAILERS* ANÓNIMOS

M es mi mensaje real; [M, K] significa «mensaje M encriptado usando la clave K». Kr es la clave pública del receptor al que va dirigido mi mensaje, Er es su dirección de correo electrónico. Voy a emplear un total de tres*remailers*; sus claves públicas son K1, K2, K3, y sus direcciones de correo son E1, E2, E3. Lo que mando al primer*remailer* es:

[([([([M, Kr] + Er), K3] + E3), K2] + E2), K1]

El primer *remailer* emplea su clave privada para quitar la capa de arriba de la encriptación, con lo que lo deja con:

[([([M, Kr] + Er), K3] + E3), K2] + E2

Ahora puede leer E2, la dirección de correo electrónico del segundo *remailer*, así que manda el resto del mensaje a esa dirección. El segundo *remailer* recibe:

[([([M, Kr] + Er), K3] + E3), K2]

y emplea su clave privada para quitar una capa de encriptación, lo que lo deja con:

[([M, Kr] + Er), K3] + E3

Entonces manda al segundo *remailer*:

[([M, Kr] + Er), K3]

El tercer *remailer* quita la tercera capa de encriptación, lo que le da:

[M, Kr] + Er

y manda [M, Kr] al receptor al que va dirigido a Er, que entonces utiliza su clave privada para quitar el último nivel de encriptación, lo que le proporciona M, el mensaje original.

BIBLIOGRAFÍA

al-Baari, Fath. *Sahih al-Bukhari*, siglo IX (La cita es de una traducción alojada aquí:

http://members.tripod.com/safia71/pictures.htm.)

Anderson, Poul. 1962. *The Makeshift Rocket*, New York: Ace.

Ariosto, Ludovico: *Orlando furioso.* Barcelona: Lumen [España], 1986

Baker, R. R., and Bellis, M. A. 1992. "Human Sperm Competition: Infidelity, the Female Orgasm and Kamikaze Sperm." Trabajo enviado al Cuarto Encuentro Anual del Comportamiento Humano y Sociedad Evolutiva, Albuquerque, NM, julio 22–26, 1992.

Baker, R. R., and Bellis, M. A. 1994. *Human Sperm Competition: Copulation,Masturbation and Infidelity*. London: Chapman & Hall.

Barkow, Jerome H., Cosmides, Leda, and Tooby, John. 1992. *The Adapted Mind*: *Evolutionary Psychology and the Generation of Culture*. Oxford: Oxford University Press.

Benson, Bruce. 1989. "The Spontaneous Evolution of Commercial Law," *Southern Economic Journal*, Vol. 55, No. 3, pp. 644–661.

Benson, B. L. 1998. "Evolution of Commercial Law." In P. Newman, (ed.). *The New Palgrave Dictionary of Economics and the Law*, London: Macmillan Press.

Benson, B. L. 1998. "Law Merchant," In P. Newman, (ed.). *The New Palgrave Dictionary of Economics and the Law*, London: Macmillan Press.

Blackstone,William. 1979. *Commentaries on the Laws of England*, first ed. 1765–1769, Facsimile from University of Chicago Press.

Bodde, Dirk and Morris, Clarence. 1973. *Law in Imperial China*. Philadelphia: University of Pennsylvania Press.

Bredart, Serge and French, Robert M. 1999. "Do Babies Resemble Their Fathers More Than Their Mothers? A Failure to Replicate Christenfeld & Hill (1995)." *Evolution and Human Behavior*, Vol. 20, No. 3, pp. 129–135.

Buchanan, James M.; Tullock, Gordon: *El cálculo del consenso: fundamentos lógicos de la democracia constitucional.* Madrid: Espasa-Calpe, 1980.

Buckley, William F. 2000. *Let Us Talk of Many Things: The Collected Speeches with New Commentary by the Author*. Forum. pp. xxii–xxiii. Rocklin: Prima Lifestyles.

Buss, David M. 2000. *The Dangerous Passion:Why Jealousy Is as Necessary as Love and Sex*. London: Bloomsbury Publishing.

Buss, David M. 2004. *Evolutionary Psychology: The New Science of the Mind*. Boston: Pearson.

Casanova di Seingalt, Giacomo Girolamo: *Historia de mi vida.* Barcelona: Libros y Publicaciones Periódicas, 1984

Castronovo, Edward. 2006. *Synthetic Worlds*. Chicago: University of Chicago Press.

Christenfeld, N. and Hill, E. 1995. "Whose Baby Are You?" *Nature*, Vol. 378,
p. 669.

Clarke, Arthur. 1981. "The Space Elevator: 'Thought Experiment', or Key to the Universe." En *Advances in Earth Oriented Applied Space Technologies*, Vol. 1. London: Pergamon Press.

Daly, Martin and Wilson, Margo. 1988. *Homicide*. New York: Aldine de Gruyter.

Daly, Martin and Wilson, Margo. 1992. "The Man Who Mistook His Wife for a
Chattel." In *The Adapted Mind*, pp. 292–297.

Davies, Stephen. 2002. "The Private Provision of Police during the Eighteenth and Nineteenth Centuries," in *The Voluntary City: Choice, Community, and Civil
Society*, ed. David T. Beito, Peter Gordon, and Alexander Tabarrok. Ann Arbor:
University of Michigan Press.

Dawkins, Richard: *El relojero ciego.* Barcelona: RBA, 2004

Diamond, Jared: "El peor error de la historia de la especie humana". 1987
En
http://www.ua.es/personal/fernando.ballenilla/Apuntes/El_peor_error_de_la_historia_de%20_la_especie_humana_Jared_Diamond.pdf

Drexler, K. Eric: *La nanotecnología: el surgimiento de las máquinas de creación*. Barcelona: Gedisa, 1993

Faille, Christopher. 2007. “Trading on Reputation: Stateless Justice in the Medieval Mediterranean.” *Reason Magazine*, January, pp. 66–69.

Feynman, Richard: “Hay bastante espacio en el fondo". 1960 En http://es.scribd.com/doc/118981369/Hay-Bastante-Espacio-en-el-Fondo-There%C2%B4s-Plenty-of-Room-at-the-Botttom-Richard-P-Feynman-Traduccion-Pablo-Martin-Aguero.

Fisher, Helen E.: *Por qué amamos: naturaleza y química del amor romántico.* Madrid: Taurus, 2004.

Flinn, Mark. 1988. “Parent–Offspring Interactions in a Caribbean Village: Daughter Guarding.” In *Human Reproductive Behaviour: A Darwinian Perspective*, eds. L. Betzig, M. Borgerhoff Mulder, y P. Turke, pp. 189–200. Cambridge: Cambridge University Press.

Foldvary, Fred E., y Klein, Daniel B. eds. 2003. *The Half-Life of Policy Rationales: How New Technology Affects Old Policy Issues*. New York: NYU Press.

Freeman, Derek. 1983. *Margaret Mead and Samoa: The Making and Unmaking of an Anthropological Myth*. Cambridge: Harvard University Press.

Freitas, Robert. 1985. “Can the Wheels of Justice Turn for Our Friends in the Mechanical Kingdom? Don’t Laugh. . . . ” *Student Lawyer*, 13(January), pp. 54–56.

Freitas, Robert. 1999. *Nanomedicine*, Vol. I: Basic Capabilities. Austin: Landes Bioscience.

Freitas, Robert A. Jr. 1998. “Exploratory Design in Medical Nanotechnology: A

Mechanical Artificial Red Cell,” *Artificial Cells, Blood Substitutes, and Immobilization Biotechnology*, 26 (4), pp. 411–430.

Freitas,Robert A. Jr. 2000. “Some Limits to Global Ecophagy by Biovorous Nanoreplicators, with Public Policy Recommendations,” Foresight Institute, April.

Friedman, D. 1972. “Laissez-Faire in Population: The Least Bad Solution,” New York: Population Council. (Occasional Paper).

Friedman, D.: *La maquinaria de la libertad*. Innisfree (versión Kindle), 1973.

Friedman, D. 1979. “Private Creation and Enforcement of Law – A Historical Case.” *Journal of Legal Studies* Vol. 8, No. 2 (March), pp. 399–415.
Friedman, David D.: *Teoría de los precios*. Madrid: Centro de Estudios Superiores Sociales y Jurídicos Ramón Carrande, 1992.
Friedman, D. 1994. “A Positive Account of Property Rights,” *Social Philosophy and Policy*, Vol. 11,No. 2 (Summer), pp. 1–16.
Friedman, D. 1995. “Making Sense of English Law Enforcement in the Eighteenth Century,” *The University of Chicago Law School Roundtable* (Spring/Summer), pp. 475–505.
Friedman, D. 1996. *Hidden Order: The Economics of Everyday Life*. New York: Collins.
Friedman, D. 2000. “Privacy and Technology.” In *The Right to Privacy*, ed. Ellen Frankel Paul, Fred D. Miller, Jr., and Jeffrey Paul. Cambridge: CambridgeUniversity Press.
Friedman, D. 2001. *Law's Order: What Economics Has to Do with Law and Why It Matters*. Princeton: Princeton University Press.
Friedman, D. 2005. “From Imperial China to Cyberspace: Contracting without the State,” *Journal of Law, Economics, and Policy* 1, pp. 349–370.
Gass, S. I. and Garille, S. 2001. “Stigler's Diet Problem Revisited.” *Operations Research*, Vol. 49, No. 1, pp. 1–13.
Greif, Avner. 2006. *Institutions and the Path to the Modern Economy: Lessons from Medieval Trade*. New York: Cambridge University Press.
Hanson, Robin. 1994. “Can Wiretaps Remain Cost Effective?” *Communications of the ACM*, December.
Heinlein, Robert. 1948. *Beyond This Horizon*. Reading: Fantasy Press.
Heinlein, Robert. 1950. *Waldo and Magic*, Inc. Garden City: Doubleday.
Heinlein, Robert Anson: *La luna es una cruel amante.* Barcelona: Acervo, 1992.
Hirschleifer, J. 1971. “The Private and Social Value of Information and the Reward to Inventive Activity.” *American Economic Review*, Vol. 61, No. 3, pp. 562–574.
Hollander, Lee M. tr. 1988. *Saga of the Jomsviking*. Austin: University of Texas Press.

Klein, Daniel B. ed. 1997. *Reputation: Studies in the Voluntary Elicitation of Good Conduct, Ann Arbor*: University of Michigan Press.

Knoll, Andrew H. 2004. *Life on a Young Planet: The First Three Billion Years of Evolution on Earth*. Princeton: Princeton University Press.

Levin, Ira: *Los niños del Brasil*. Barcelona: Pomaire, 1978.

Lewis, Clive Staples: *El gran divorcio*. Madrid: Rialp, 1997.

Mann, Charles C. 2005. 1491: *New Revelations of the Americas before Columbus*, New York: Knopf.

McNeill, William H.: *Plagas y pueblos*. Madrid: Siglo XXI de España, 1984.

Meadows, Donella H.; et al.: *Más allá de los límites del crecimiento* / Schvartz, Carlos Alberto / Madrid: Aguilar [España], 1993.

Medawar, P. B. 1946. "Old Age and Natural Death." *Modern Quarterly* 1, pp. 30–56.

Mehlman, Maxell J., Benger, Elizabeth, and Wright, Matthew M. 2005. "Doping in Sports and the Use of State Power," *Saint Louis University Law Journal*, Vol. 50,

No. 1, Fall, pp. 15–73.

Mencken, H. L.: *En defensa de las mujeres*. Madrid: La Fábrica, 2003.

Mueller, Dennis Cary: *Elección pública.* Madrid: Alianza Editorial, 1984

Niven, Larry. 1969. *The Shape of Space*. New York: Ballantine.

Niven, Larry. 1973. *Protector*. New York: Ballantine.

Nozick, Robert: *Anarquía, estado y utopía*. Fondo de Cultura Económica, 1988

Oldstone, Michael B. A. 1998. *Viruses, Plagues, and History*. Oxford: Oxford

University Press.

Orwell, George: *1984.* Barcelona: s. n., 1977.

Orwell, Sonia and Angus, Ian eds. 1968. *The Collected Essays, Journalism and Letters of George Orwell*. Volume III. New York: Harcourt Brace Jovanovich.

Parker, Don B. 1983. *Fighting Computer Crime*. New York: Scribner.

Pinker, Steven: *La tabla rasa : la negación moderna de la naturaleza humana.* Barcelona: Paidós Ibérica, 2003.

Posner, Richard. 1978. "An Economic Theory of Privacy," *Regulation*, May/June, pp. 19–26.

Posner, Richard. 1978. “The Right of Privacy,” *Georgia Law Review*, Vol. 12, No. 3 (Spring), pp. 393–428.

Read, Leonard. 1958. “Yo, el lápiz”. En http://www.hacer.org/pdf/Lapiz.pdf

Ridley, Matt: *Genoma: la autobiografía de una especie en 23 capítulos.* Madrid: Taurus, 2000.

Ridley, Matt. 1995. *The Red Queen*: Sex *and the Evolution of Human Nature*. New York: Penguin.

Rosen, Winifred; Weil, Andrew: *Del café a la morfina: todo lo que necesita saber sobre las sustancias psicoactivas, de la .A. a la .Z.* Barcelona: RBA, 1999

Savulescu, J., Foddy, B., and Clayton, M. 2004. “Why We Should Allow Performance Enhancing Drugs in Sport.”*British Journal of Sports Medicine*, Vol. 38, No. 6, pp. 666–670.

Sayers, Dorothy. 1947. *Unpopular Opinions*. New York: Harcourt Brace.

Scheck, Barry, Neufeld, Peter, and Dwyer, Jim. 2000. *Actual Innocence: Five Days to Execution, and Other Dispatches from the Wrongly Convicted*. NewYork: Doubleday.

Schneier, Bruce. 1994. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken: Wiley.

Schulman, J. Neil. 1983. *The Rainbow Cadenza*. New York: Simon & Schuster.

Silver, Lee M.: *Vuelta al Edén: más allá de la clonación en un mundo feliz.* Madrid: Taurus, 1998.

Spencer, N. A., McClintock, M. K., Sellergren, S. A., Bullivant, S., Jacob. S., and Mennella, J. A. 2004. “Social Chemosignals from Breastfeeding Women Increase Sexual Motivation,” *Hormones and Behavior*, Vol. 46, No. 3, pp. 362–370.

Stephenson, Neal: *Snow crash*. Barcelona: Gigamesh 2000.

Sterling, Bruce. 1992. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam.

Sterling, Bruce: *El fuego sagrado*. Barcelona: Ediciones B, 1998

Stiegler, Marc. 1999. *Earthweb*. Riverdale: Baen.

Stigler, G. 1945. “The Cost of Subsistence,” *Journal of Farm Economics*, Vol. 25, No. 2, pp. 303–314.

Stout, Rex. 1948. *“And Be a Villain.”* New York: Viking.

Timmons, C. Robin and Hamilton, Leonard W. 1990. *Principles of Behavioral Pharmacology*. Upper Saddle River: Prentice Hall.

Vinge, Vernor. 1987. *True Names . . . and Other Dangers*. Riverdale: Baen.

Viscusi, W. Kip. 1991. *Reforming Products Liability*. Cambridge: Harvard University Press.

White, Lawrence H. 1995. *Free Banking in Britain: Theory, Experience and Debate,* 1800–1845. London: Institute for Economic Affairs.

Williamson, Oliver E. 1983. *Markets and Hierarchies: Analysis and Antitrust Implications*. New York: Free Press.

Wright, Robert. 1994. *The Moral Animal: Evolutionary Psychology and Everyday Life*. New York: Vintage.